MS221 HB

The Open University

EXPLORING MATHEMATICS

Handbook

HANDBOOK

The Open University

EXPLORING MATHEMATICS

Handbook

Prepared by the course team

HANDBOOK

About this course

This course, MS221 *Exploring Mathematics*, and the courses MU120 *Open Mathematics* and MST121 *Using Mathematics* provide a flexible means of entry to university-level mathematics. Further details may be obtained from the address below.

MS221 uses the software program Mathcad (MathSoft, Inc.) to investigate mathematical concepts and as a tool in problem solving. This software is provided as part of the course.

This publication forms part of an Open University course. Details of this and other Open University courses can be obtained from the Student Registration and Enquiry Service, The Open University, PO Box 197, Milton Keynes, MK7 6BJ, United Kingdom: tel. +44 (0)870 333 4340, e-mail general-enquiries@open.ac.uk

Alternatively, you may visit the Open University website at http://www.open.ac.uk where you can learn more about the wide range of courses and packs offered at all levels by The Open University.

To purchase a selection of Open University course materials, visit the webshop at www.ouw.co.uk, or contact Open University Worldwide, Michael Young Building, Walton Hall, Milton Keynes, MK7 6AA, United Kingdom, for a brochure: tel. +44 (0)1908 858785, fax +44 (0)1908 858787, e-mail ouwenq@open.ac.uk

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 1997. New edition 2004. Reprinted with corrections 2004, 2005.

Edited, designed and typeset by The Open University, using the Open University TEX System.

Printed and bound in the United Kingdom by The Charlesworth Group, Huddersfield.

ISBN 0 7492 6647 3

5.3

Contents

The MS221 Handbook includes the entries from the MST121 Handbook, as well as the entries for MS221.

If you are taking MST121 and MS221 together, then we suggest that you use the MS221 Handbook for both courses. You are allowed to annotate this combined handbook, and to take it into the examination (with the MST121 Handbook, if you wish).

The Greek alphabet

A	α	alpha	N	ν	nu
B	β	beta	Ξ	ξ	xi
Γ	γ	gamma	O	o	omicron
Δ	δ	delta	Π	π	pi
E	ε	epsilon	P	ρ	rho
Z	ζ	zeta	Σ	σ	sigma
H	η	eta	T	τ	tau
Θ	θ	theta	Y	υ	upsilon
I	ι	iota	Φ	ϕ	phi
K	κ	kappa	X	χ	chi
Λ	λ	lamda	Ψ	ψ	psi
M	μ	mu	Ω	ω	omega

SI units

The International System of units (SI units) is an internationally agreed set of units and symbols for measuring physical quantities.

Some of these are base units, such as

metre	symbol	m	(measurement of length),
second	symbol	s	(measurement of time),
kilogram	symbol	kg	(measurement of mass).

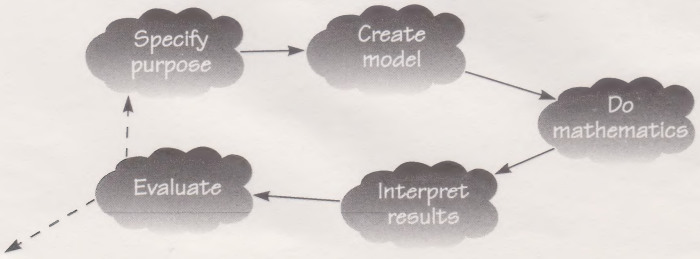
Prefixes may be added to units. Commonly used prefixes are

c	centi	or	10^{-2}	(e.g. centimetre, cm),
m	milli	or	10^{-3}	(e.g. millisecond, ms),
μ	micro	or	10^{-6}	(e.g. microsecond, μs),
k	kilo	or	10^{3}	(e.g. kilogram, kg),
M	mega	or	10^{6}	(e.g. megagram, Mg).

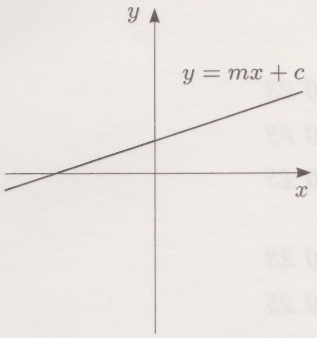
There are also derived units, which are used for quantities whose measurement combines base units in some way. Some of these are

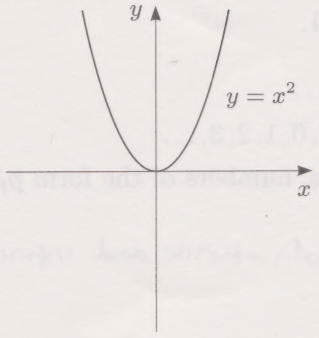
area	m^2	(metres squared or square metres),
volume	m^3	(metres cubed or cubic metres),
velocity	$\mathrm{m\,s}^{-1}$	(metres per second),
acceleration	$\mathrm{m\,s}^{-2}$	(metres per second per second).

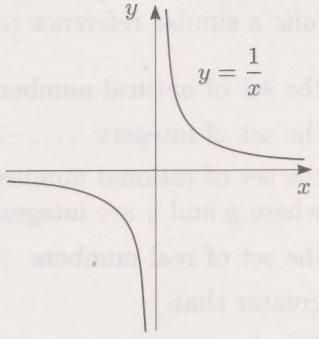
Mathematical modelling

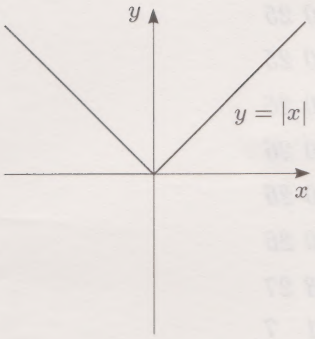


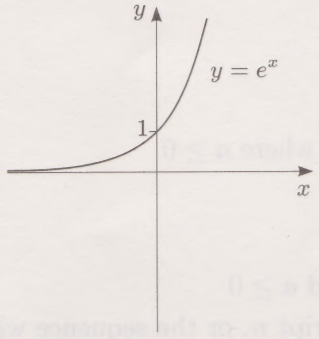
Some useful graphs

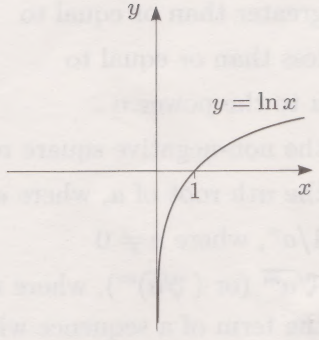


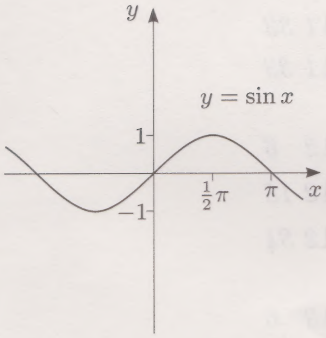


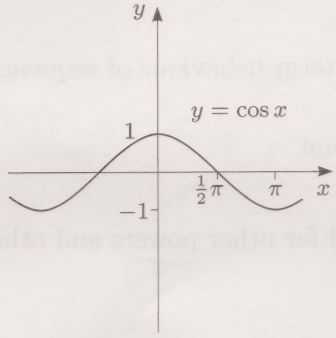


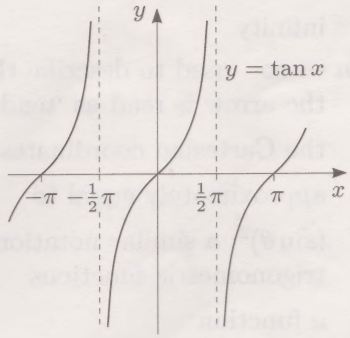


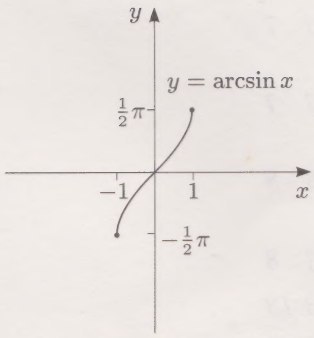


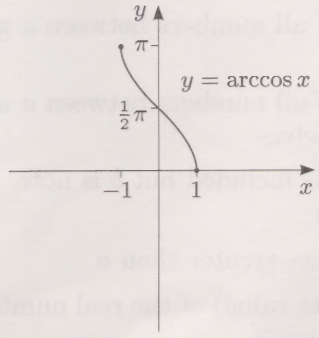


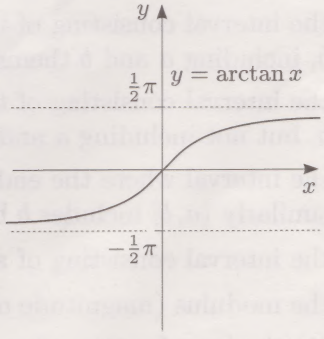












Notation

Some of the notation used in MST121 and MS221 is listed below. The right-hand column gives in **bold** the chapter and page of MS221 where the notation is first used, or in *italic* a similar reference to MST121.

$\mathbb{N}$	the set of natural numbers: $1, 2, 3, \ldots$	*A0 23*
$\mathbb{Z}$	the set of integers: $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$	*A0 23*
$\mathbb{Q}$	the set of rational numbers, that is, numbers of the form p/q where p and q are integers, $q \neq 0$	*A0 23*
$\mathbb{R}$	the set of real numbers (decimals - finite and infinite)	*A0 23*
$>$	greater than	*A0 25*
$<$	less than	*A0 25*
$\geq$	greater than or equal to	*A0 25*
$\leq$	less than or equal to	*A0 25*
a^n	a to the power n	*A0 26*
$\sqrt{a}$	the non-negative square root of a, where $a \geq 0$	*A0 26*
$\sqrt[n]{a}$	the nth root of a, where $a \geq 0$	*A0 26*
a^{-n}	$1/a^n$, where $a \neq 0$	*A0 26*
$a^{m/n}$	$\sqrt[n]{a^m}$ (or $(\sqrt[n]{a})^m$), where $n > 0$ and $a \geq 0$	*A3 27*
a_n	the term of a sequence with subscript n, or the sequence whose general term is a_n	*A1 7*
∞	infinity	*A1 33*
$a_n \to l$ as $n \to \infty$	used to describe the long-term behaviour of sequences; the arrow is read as 'tends to'	*A1 33*
(x, y)	the Cartesian coordinates of a point	*A2 6*
$\simeq$	approximately equal to	*A2 18*
$\sin^2\theta$	$(\sin\theta)^2$; a similar notation is used for other powers and other trigonometric functions	*A2 34*
f	a function	*A3 6*
$f(x) = \ldots$	specifies (in terms of x) the rule of the function f	*A3 6*
$[a, b]$	the interval consisting of the set of all numbers between a and b, including a and b themselves	*A3 7*
(a, b)	the interval consisting of the set of all numbers between a and b, but not including a and b themselves	*A3 7*
$[a, b)$	the interval where the endpoint a is included but b is not; similarly $(a, b]$ includes b but not a	*A3 8*
(a, ∞)	the interval consisting of all numbers greater than a	*A3 8*
$\lvert x \rvert$	the modulus (magnitude or absolute value) of the real number x	*A3 13*
e	(1) the base for the natural logarithm function and the exponential function; $e = 2.718\,281\ldots$	*A3 33*
	(2) the eccentricity of a conic	**A2 26**
exp	the exponential function	*A3 34*
f^{-1}	the inverse function of the one-one function f	*A3 37*
$\arccos x$	the angle in the interval $[0, \pi]$ whose cosine is x	*A3 41*

$\arcsin x$	the angle in the interval $[-\frac{1}{2}\pi, \frac{1}{2}\pi]$ whose sine is x	*A3 40*
$\arctan x$	the angle in the interval $(-\frac{1}{2}\pi, \frac{1}{2}\pi)$ whose tangent is x	*A3 41*
$\log_a$	the logarithm function to the base a	*A3 42*
ln	the natural logarithm function, that is, $\log_e$ where $e = 2.718\,281\ldots$	*A3 44*
ϕ	the value of the golden ratio, given by the positive solution of the equation $x^2 - x - 1 = 0$	**A1 10**
Pd	the perpendicular distance from the point P to the line d	**A2 21**
$\longmapsto$	'maps to' for variables; used to specify the rule of a function, for example, $x \longmapsto e^x$	**A3 6**
$\longrightarrow$	'maps to' for sets; used in functions to show the domain mapping to the codomain, for example, $[0, 4] \longrightarrow [0, 16]$	**A3 6**
$\mathbb{R}^2$	the Cartesian plane, that is, the set of points (x, y) where x and y are real numbers	**A3 7**
$f(A)$	the set of all images $f(x)$ with x in A for the function f	**A3 9**
$t_{p,q}$	the translation function that moves each point p units to the right and q units up	**A3 16**
r_θ	the rotation function that rotates each point through an angle θ anticlockwise about the origin	**A3 19**
q_θ	the reflection function that reflects each point in the line through the origin, which makes an angle θ measured anticlockwise from the positive x-axis	**A3 23**
$g \circ f$	the composite of the isometries g and f (f first, then g)	**A3 25**
$\sum_{i=1}^{n} a_i$	the sum $a_1 + a_2 + \cdots + a_n$	*B1 11*
$\lim_{n\to\infty} a_n$	the limit of the convergent sequence a_n	*B1 42*
$\sum_{i=1}^{\infty} a_i$	the infinite sum $a_1 + a_2 + \cdots$	*B1 48*
$\mathbf{A}$	a matrix	*B2 19*
$\mathbf{AB}$	the product of the matrices $\mathbf{A}$ and $\mathbf{B}$	*B2 19*
$\mathbf{A}^n$	the nth power of the square matrix $\mathbf{A}$	*B2 21*
$\mathbf{A} + \mathbf{B}$	the sum of the matrices $\mathbf{A}$ and $\mathbf{B}$	*B2 22*
$k\mathbf{A}$	the scalar multiple of the matrix $\mathbf{A}$ by the real number k	*B2 23*
$\mathbf{A} - \mathbf{B}$	the difference of the matrices $\mathbf{A}$ and $\mathbf{B}$	*B2 23*
a_{ij}	the element in the ith row and jth column of the matrix $\mathbf{A}$	*B2 24*
$\mathbf{v}$	a vector	*B2 26*
v_i	the ith component of the vector $\mathbf{v}$	*B2 26*
$\mathbf{I}$	the identity matrix	*B2 35*
$\mathbf{A}^{-1}$	the inverse of the invertible matrix $\mathbf{A}$	*B2 36*
$\det \mathbf{A}$	the determinant of the square matrix $\mathbf{A}$	*B2 38*
$\mathbf{Ax} = \mathbf{b}$	the matrix form of a pair of simultaneous linear equations	*B2 41*
$\mathbf{i}$	the Cartesian unit vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	*B3 8*
$\mathbf{j}$	the Cartesian unit vector $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	*B3 8*

$\mathbf{0}$	the zero vector	*B3 8*
$\lvert\mathbf{a}\rvert$	the magnitude of the vector $\mathbf{a}$	*B3 10*
$\overrightarrow{PQ}$	the displacement vector from P to Q	*B3 12*
$\overrightarrow{OQ}$	the position vector of Q	*B3 12*
$\mathbf{a} = a_1\mathbf{i} + a_2\mathbf{j}$	the component form of the vector $\mathbf{a}$	*B3 16*
g	the magnitude of the acceleration due to gravity	*B3 40*
$\mathbf{W}$	weight (a vector)	*B3 40*
$\mathbf{T}$	tension (a vector)	*B3 41*
$\mathbf{N}$	normal reaction (a vector)	*B3 41*
$\in$	belongs to (in)	**B1 6**
$\subseteq$	is a subset of	**B1 6**
$f'(x)$	the gradient of the smooth function f at the point $(x, f(x))$	**B1 21**
$g \circ f$	the composite function with rule $x \longmapsto g(f(x))$	**B1 33**
f^p	the pth iterate of the function f	**B1 39**
$n!$	n factorial	**B1 42**
${}^nP_k$	the number of permutations of n objects taken k at a time	**B1 44**
${}^nC_k$	the number of combinations of n objects taken k at a time	**B1 45**
$\mathbf{p}$	the position vector of the point P	**B2 9**
$\mathbf{R}_\theta$	the matrix representing the rotation r_θ	**B2 11**
$\mathbf{Q}_\theta$	the matrix representing the reflection q_θ	**B2 13**
$\max\{a, b\}$	the maximum of two real numbers a and b	**B3 45**
f'	the (first) derived function of f	*C1 13*
$f'(x)$	the (first) derivative of the function f at the point x	*C1 13*
f''	the second derived function of f	*C1 28*
$f''(x)$	the second derivative of the function f at the point x	*C1 28*
$f^{(n)}(x)$	the nth derivative of the function f at the point x	**C1 16**
$\dfrac{dy}{dx}$	the (first) derivative of y with respect to x (Leibniz notation)	*C1 41*
$\dfrac{d^2y}{dx^2}$	the second derivative of y with respect to x (Leibniz notation)	*C1 42*
$\dfrac{d}{dx}(y)$	a variation of $\dfrac{dy}{dx}$	*C1 43*
$\dfrac{d}{dx}(f(x))$	a variation of the Leibniz notation for $f'(x)$	*C1 43*
$\dot{s}$	the (first) derivative of s with respect to t, where t is time (Newton's notation)	*C1 43*
$\ddot{s}$	the second derivative of s with respect to t, where t is time (Newton's notation)	*C1 43*
$\int f(x)\,dx$	the indefinite integral of $f(x)$ with respect to x	*C2 8*
$\int f$	the indefinite integral of the function f	*C2 8*
$\int_a^b f(x)\,dx$	the definite integral of $f(x)$ from a to b	*C2 41*

$\int_a^b f$	the definite integral of the function f from a to b	*C2 41*
$[F(x)]_a^b$	$F(b) - F(a)$	*C2 41*
$y(a) = b$	shorthand for the initial condition $y = b$ when $x = a$	*C3 10*
$x \to \pm\infty$	shorthand for $x \to \infty$ and $x \to -\infty$	**C1 35**
$p_n(x)$	a Taylor polynomial of degree n for a given function f	**C3 23**
$\sinh x$	the hyperbolic sine function (pronounced 'shine' or 'sine-sh')	**C3 40**
$\cosh x$	the hyperbolic cosine function (pronounced 'cosh')	**C3 40**
$P(E)$	the probability that the event E occurs	*D1 10*
$P(X = j)$	the probability that a random variable X takes the value j	*D1 37*
μ	the mean of a probability distribution, or a population mean	*D1 43* *D2 23*
$\overline{x}$	the sample mean	*D2 21*
s	the sample standard deviation	*D2 25*
σ	the standard deviation of a probability distribution, or a population standard deviation	*D2 24*
SE	a standard error, that is, the standard deviation of a sampling distribution	*D3 14* *D4 20*
ESE	an estimated standard error	*D4 22*
$Q1$	the lower quartile	*D4 9*
$Q3$	the upper quartile	*D4 9*
H_0	the null hypothesis of a hypothesis test	*D4 18*
H_1	the alternative hypothesis of a hypothesis test	*D4 18*
$\mathbb{C}$	the set of complex numbers	**D1 11**
i	$\sqrt{-1}$	**D1 11**
$\mathrm{Re}(z)$	the real part of the complex number z	**D1 11**
$\mathrm{Im}(z)$	the imaginary part of the complex number z	**D1 11**
$\overline{z}$	the complex conjugate of the complex number z	**D1 19**
$\lvert z \rvert$	the modulus of the complex number z	**D1 26**
$\arg(z)$	an argument of the complex number z	**D1 26**
$\langle r, \theta \rangle$	the polar form of a complex number, where r is its modulus and θ is an argument	**D1 25**
$[x]$	the greatest integer that is less than or equal to x	**D2 8**
$\equiv$	'congruent to' (with respect to a particular modulus)	**D2 9**
$\mathbb{Z}_n$	the set $\{0, 1, 2, \ldots, n-1\}$	**D2 21**
$\mathbb{Z}_n^*$	the set $\{1, 2, \ldots, n-1\}$	**D3 26**
$+_n$	the operation of addition in $\mathbb{Z}_n$	**D2 21**
$\times_n$	the operation of multiplication in $\mathbb{Z}_n$	**D2 21**
$S(X)$	the set of symmetries of a plane set X	**D3 12**
$\mathbb{C}^*$	the set of non-zero complex numbers	**D3 23**
$\mathbb{Q}^*$	the set of non-zero rational numbers	**D3 23**
$\mathbb{R}^*$	the set of non-zero real numbers	**D3 23**
$(G, *)$	the group consisting of the set G and the operation $*$	**D3 22**

$\lvert G\rvert$	the order of the group $(G, *)$	**D3 24**
$A \cup B$	the set consisting of all the elements of the set A and all the elements of the set B	**D3 29**
$\wedge$	the operation 'and' for combining propositions	**D4 20**
$\vee$	the operation 'or' for combining propositions	**D4 22**
$\Rightarrow$	the operation 'if ... then' for combining propositions	**D4 21**
$\Leftrightarrow$	the operation 'if and only if' for combining propositions	**D4 25**

Glossary

Below is a glossary of terms used in MST121 and MS221. First a definition of the term is given, and then a page in this handbook where more detail can be found. Finally, the chapter and page of MS221 where the term is first used is given in **bold**, or a similar reference to MST121 is given in *italic*.

Abelian group See *commutative group.*

absolute value (of a real number) See *modulus (of a real number x).*

acceleration The rate of change of velocity. *B3 40*

acceleration due to gravity The magnitude, g, of the acceleration with which an object falls. On Earth, $g = 9.8$ m s^{-2}. *B3 40*

affine transformation A function with domain and codomain $\mathbb{R}^2$, and rule of the form $\mathbf{x} \longmapsto \mathbf{Ax} + \mathbf{a}$, where $\mathbf{A}$ is a 2×2 matrix and $\mathbf{a}$ is a vector with two components. 61 **B2 49**

alternating digit sum The alternating digit sum of a positive integer is the sum of the odd-placed digits (starting from the units digit) minus the sum of the even-placed digits. For example, the alternating digit sum of 2941 is $1 - 4 + 9 - 2 = 4$. 82 **D2 16**

alternative hypothesis The hypothesis that is accepted at the end of a hypothesis test when the null hypothesis is rejected. 78 *D4 18*

and The operation $\wedge$ used to combine propositions. 87 **D4 20**

antiderivative See *integral (of a function $f(x)$ over I).*

arbitrary constant See *constant of integration.*

arccosine The inverse function of the cosine function with domain restricted to $[0, \pi]$. 43 *A3 41*

arcsine The inverse function of the sine function with domain restricted to $[-\frac{1}{2}\pi, \frac{1}{2}\pi]$. 43 *A3 40*

arctangent The inverse function of the tangent function with domain restricted to $(-\frac{1}{2}\pi, \frac{1}{2}\pi)$. 43 *A3 41*

Argand diagram A representation of the set of complex numbers as a plane, with $z = x + yi$ represented as the point (x, y). **D1 23**

argument (of a complex number) For $z = a + bi$, any θ satisfying $\cos\theta = a/|z|$ and $\sin\theta = b/|z|$ is an argument of z (written $\arg(z)$). 79 **D1 26**

arithmetic mean The arithmetic mean (or average) of a set of n numbers is the sum of the numbers divided by n. *A1 14*

arithmetic sequence A sequence in which each term (apart from the first) is obtained by adding a fixed number to the previous term. 40 *A1 14*

associative operation An operation $*$ on a set X is associative if $(a * b) * c = a * (b * c)$ for all a, b and c in X. **D1 14**

asymptote A line which a curve approaches (arbitrarily closely) far from the origin. 46 *A3 11*

asymptotic behaviour For a function f, the behaviour of points on the graph of $y = f(x)$ for which the variable x or the variable y take arbitrarily large values. 66 **C1 34**

attracting 2-cycle A 2-cycle a, b of a smooth function f for which $|f'(a)f'(b)| < 1$. 57 **B1 36**

attracting fixed point A fixed point a of a smooth function f for which $|f'(a)| < 1$. 56 **B1 24**

batch size The number of values in a batch of data. 77 *D4 9*

bearing A direction given as either North or South followed by an angle (up to 90°) towards the East or West. *B3 24*

bimodal See *mode.*

binomial coefficient A number of the form ${}^nC_k$. 58 **B1 46**

binomial expansion The expansion of a binomial expression of the form $(a + b)^n$. 58 **B1 41**

binomial series The Taylor series about 0 for the function $(1 + x)^\alpha$, where α is any real number. 73 **C3 32**

bounded set A bounded set in $\mathbb{R}^2$ is a set that lies entirely within some circle. An unbounded set is a set that is not bounded. **D3 10**

boxplot A diagram consisting of a box and whiskers, which displays the median, the quartiles and the minimum and maximum values in a batch of data. 77 *D4 8*

calculus The branch of mathematics which includes the study of differentiation and integration. *C1 4*

carrying capacity See *equilibrium population level.*

Cartesian coordinate system Cartesian coordinates (x, y) specify the position of a point in a plane relative to two perpendicular axes, the x-axis (horizontal) and the y-axis (vertical). *A2 6*

Cartesian form (of a complex number) The form $z = a + bi$, where (a, b) are the Cartesian coordinates of the complex number z in an Argand diagram. 79 **D1 25**

Cartesian unit vectors The vectors $\mathbf{i} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\mathbf{j} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. 54 *B3 16*

Cayley table A table showing the composites of pairs of elements of a finite group. 85 **D3 15**

centre of a Taylor series The point about which the Taylor series is constructed. 73 **C3 30**

centre (of an ellipse or hyperbola) The point of intersection of the axes of symmetry of the conic (the lines in which the conic is symmetric). **A2 14**

chaotic sequence A sequence displaying apparently unstructured behaviour. 50 *B1 40*

characteristic equation The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has characteristic equation $k^2 - (a + d)k + ad - bc = 0$. 62 **B3 19**

chord A line segment joining two points on a curve. **B1 20**

cipher A function applied to the characters of a message. 83 **D2 32**

ciphertext The image of a message under a cipher. 83 **D2 32**

circle The set of points in a plane that are a fixed distance from a specified point in the plane. 41 *A2 20*

closed form A formula that defines a sequence a_n in terms of the subscript n. It should be accompanied by a statement of the appropriate range for n. 40 *A1 8*

closed operation An operation $*$ on a set A is closed if whenever a and b are in A, then $a * b$ is also in A. 85 **D3 19**

codomain A set containing all the outputs of a function. See also *function.* 47 **A3 6**

coefficient matrix The square matrix used when a pair of simultaneous linear equations are written in matrix form. 53 *B2 40*

coefficient (of a term) The factor by which the term is multiplied in a particular product. *A0 31*

column (of a matrix) See *matrix.*

combination (of n objects taken k at a time) A selection of k objects from n objects (all different) in which order does not matter. 58 **B1 44**

common difference The difference between any two successive terms in an arithmetic sequence. 40 *A1 14*

common factor Two positive integers a and b have a common factor c if c is a factor of both a and b. **D2 23**

common logarithm The logarithm function with base 10. *A3 44*

common ratio The ratio of any two successive terms in a geometric sequence. 40 *A1 19*

commutative group A commutative (or Abelian) group is a group with the additional property that the binary operation is commutative. 85 **D3 24**

commutative operation An operation $*$ on a set X is commutative if $a * b = b * a$ for all a and b in X. **D1 14**

completed-square form The completed-square form of $x^2 + 2px$ is $(x + p)^2 - p^2$. 41 *A2 26*

complex conjugate See *conjugate (of a complex number).*

complex number A number of the form $a + bi$, where $i = \sqrt{-1}$ and a and b are real numbers. 79 **D1 11**

complex-valued function A function with codomain $\mathbb{C}$. **D1 47**

component form (of a vector) The description of a vector $\mathbf{a}$ in terms of the Cartesian unit vectors $\mathbf{i}$ and $\mathbf{j}$: $\mathbf{a} = a_1\mathbf{i} + a_2\mathbf{j}$. 54 *B3 16*

component (of a vector) See *vector.*

composite function A function $g \circ f$ with rule $x \longmapsto g(f(x))$, where f and g are two functions which have the property that the image set of f is a subset of the domain of g. 56 **B1 33**

composite isometry An isometry $g \circ f$ obtained by performing the isometry f followed by the isometry g. 48 **A3 26**

compound proposition A proposition consisting of a combination of other propositions using operations such as $\wedge$, $\vee$ and $\Rightarrow$. 87 **D4 21**

conclusion A statement whose truth is deduced at the end of a deductive argument. **D4 16**

confidence interval An interval of plausible values for a population parameter. 77 *D3 19*

congruence A statement of the form $a \equiv b \pmod{n}$, which means that a and b have the same remainder when divided by n. 81 **D2 9**

conic sections The curves obtained as cross-sections when a double cone is sliced by a plane. See also *ellipse, hyperbola* and *parabola.* 46 **A2 9**

conjecture A general statement that may be true, but of which no proof is known. **A1 18**

conjugate (of a complex number) The conjugate of the complex number $z = a + bi$, written $\overline{z}$, is $a - bi$. 79 **D1 19**

constant (1) A significant number; for example, π. *A0 28*

constant (2) A term in a mathematical expression, whose value does not change during a particular calculation. *A1 14*

constant function A function f with rule of the form $f(x) = c$, where c is a constant. *C1 35*

constant of integration The constant c in the indefinite integral $F(x) + c$. 67 *C2 8*

constant sequence A sequence in which each term has the same value. *A1 16*

constructive proof A proof which shows that something exists by constructing it explicitly. **D4 13**

continuous function Informally, a function is said to be continuous if its graph can be drawn without lifting the pen from the paper. *A3 49*

continuous model A model (or representation) in which the associated quantity or quantities can vary throughout some interval of the real line. *A3 49*

continuous variable A variable that can take any value in an interval of the real line. *A3 49*

contour The set of points, in the domain of a function f of two variables, at which f takes a particular value. 47 **A3 13**

contour plot A collection of contours for a given function. 47 **A3 13**

convergent sequence A sequence that settles down in the long term to values that are effectively constant. Such a sequence is said to converge. See also *limit (of a sequence).* 51 *B1 42*

converse (of a proposition) The converse of a proposition of the form $p \Rightarrow q$ is the proposition $q \Rightarrow p$. 87 **D4 23**

coprime If the only common factor of a and b is 1, then a and b are coprime. **D2 23**

corollary A straightforward consequence of a theorem, and often a special case of that theorem. **D2 6**

cosecant (of an angle θ) The cosecant of θ is $1/\sin\theta$, provided that $\sin\theta \neq 0$. *A2 36*

cosh x The hyperbolic cosine function. 74 **C3 40**

cosine (of an angle θ) The first coordinate of the point P on the circumference of the unit circle, centre O, where the angle between the positive x-axis and the line segment OP is θ. By convention, angles are measured positively in an anticlockwise direction from the positive x-axis. 41 *A2 33*

Cosine Rule A rule that relates three sides and one angle of a triangle. 55 *B3 34*

cotangent (of an angle θ) The cotangent of θ is $1/\tan\theta$, provided that $\tan\theta \neq 0$. *A2 36*

counter-example A example which shows that a conjecture is false. **A1 19**

cross-term In the equation of a quadratic curve, the term involving xy is called the cross-term. **A3 38**

cryptanalysis The process of breaking ciphers. **D2 32**

cryptography The process of designing ciphers. 83 **D2 32**

cubic expression An expression of the form $ax^3 + bx^2 + cx + d$, where $a \neq 0$. *A3 47*

cyclic group A cyclic group of order n is a group that comprises the n powers of a single element (called a generator of the group). **D3 42**

cycling (of a sequence) The behaviour of a sequence that takes a number of different but repeating values; for example, in a 2-cycle the sequence settles to a pattern of alternating between two values. 50 *B1 40*

decay constant The positive constant k in the first-order differential equation $dm/dt = -km$, used to model radioactive decay. 72 *C3 26*

decipher To apply the inverse of a cipher. **D2 32**

decreasing function A real function f with the property that for all x_1, x_2 in the domain of f, if $x_1 < x_2$, then $f(x_1) > f(x_2)$. 43 *A3 36*

decreasing on an interval A function f is decreasing on an interval I if for all x_1, x_2 in I, if $x_1 < x_2$, then $f(x_1) > f(x_2)$. 56 **B1 22**

deduction A step (in a proof) in which one or more propositions are known to be true and the truth of a further proposition is deduced. **D4 26**

definite integral (of a function $f(x)$ from a to b) The definite integral of a continuous function f from a to b, denoted by $\int_a^b f(x)\,dx$, is $[F(x)]_a^b = F(b) - F(a)$, where F is any integral of f over an interval I and $a, b \in I$. 67 **C2 12**

degenerate conics Those cross-sections of a double cone which consist of a single point, two intersecting lines or a single line. **A2 9**

degree of a polynomial For a polynomial in x, the highest power of x with a non-zero coefficient. *A3 47*

dependent variable A variable whose value depends on the value of another variable (or variables). *A0 28* *D4 38*

derivative (of a function f at a point x) The gradient of the graph of f at the point $(x, f(x))$, denoted by $f'(x)$. 64 *C1 14*

derived function (of a function f) The function f' defined by the process of differentiation. 64 *C1 14*

determinant (of a matrix) The determinant of the 2×2 matrix $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\det \mathbf{A} = ad - bc$. 53 *B2 38*

deviation The deviation of a value x from the population mean μ is $x - \mu$; the deviation of a value x from the sample mean $\overline{x}$ is $x - \overline{x}$. *D2 24*

diagonal matrix A square matrix for which all the non-zero elements lie on the leading diagonal. **B2 22**

diagonalising a matrix The process of expressing a 2×2 matrix $\mathbf{A}$, which has two distinct eigenvalues, in the form $\mathbf{A} = \mathbf{PDP}^{-1}$, where $\mathbf{D}$ is a diagonal matrix. 62 **B3 30**

differentiable A function f is differentiable (or smooth) if it can be differentiated at each point of its domain. 64 **C1 8**

differential equation An equation that relates an independent variable, x say, a dependent variable, y say, and one or more derivatives of y with respect to x. 71 *C3 6*

differentiation (of a function f) The process of finding the derivative $f'(x)$. 64 *C1 14*

digit sum The digit sum of a positive integer is the sum of its digits. 82 **D2 15**

dihedral group The group of order $2n$ formed by the symmetries of a regular n-gon. **D3 42**

direct integration A method for solving differential equations of the form $dy/dx = f(x)$. 71 *C3 11*

direct proof A proof that starts with given premises and works through a series of deductions to deduce the desired conclusion. **D4 9**

direction field The association, arising from a differential equation, of a gradient with each point (x, y) in a given domain, often represented by a collection of short line segments. **C2 20** *C3 38*

direction (of a vector) The angle θ, measured anticlockwise, that an arrow representing the vector makes with the positive x-axis. 54 *B3 11*

directrix A line associated with a conic. See also *eccentricity*. 46 **A2 23**

discrete model A model (or representation) in which the associated quantity or quantities can only take separated values. *A3 49*

discrete variable A variable that can only take on values in a separated set, such as the integers. *A3 49*

displacement (vector) The displacement vector from P to Q is represented by the arrow with its tail at P and its tip at Q. *B3 12*

distance The distance of a particle from the origin is a measure of how far it is from the origin, irrespective of direction. 69 *C2 26*

divergent sequence A sequence that is not convergent. **B1 7**

divisible An integer a is divisible by an integer n if $a = qn$ for some integer q. 81 **D2 7**

divisor If a and n are integers and a is divisible by n, then n is a divisor, or factor, of a. 81 **D2 7**

domain (of a function) The set of allowable input values for a function. See also *function.* 47 **A3 6**

dominant eigenline For a matrix with two distinct non-zero eigenvalues, the dominant eigenline is the eigenline corresponding to the eigenvalue of greater magnitude (if there is one). 63 **B3 46**

dominant eigenvalue For a matrix with two distinct non-zero eigenvalues, the dominant eigenvalue is the eigenvalue of greater magnitude (if there is one). 63 **B3 46**

Dominant Eigenvalue Property The property that the points of an iteration sequence generated by a matrix representing a generalised scaling will, if the initial point is not on an eigenline, tend in the direction of the dominant eigenline. 63 **B3 46**

dominant term (of a polynomial) In the polynomial function $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $n \geq 1$ and $a_n \neq 0$, we call x^n the dominant term. **C1 34**

doubling time The time that it takes for a population to double in size from any starting value. 72 *C3 32*

eccentricity A positive constant associated with a conic. It is the ratio of the distances from a point on the conic to the focus of the conic and from that point to the directrix of the conic. 46 **A2 26**

eigenline (of a matrix A) A line through the origin on which an eigenvector of **A** lies. If **A** is an invertible matrix, then the eigenlines of **A** are invariant lines of the linear transformation represented by **A**. 62 **B3 17**

eigenvalue (of a matrix A) A real number k for which there exists a non-zero vector $\mathbf{x}$ such that $\mathbf{Ax} = k\mathbf{x}$. 62 **B3 17**

eigenvector (of a matrix A) A non-zero vector $\mathbf{x}$ for which there exists a real number k such that $\mathbf{Ax} = k\mathbf{x}$. 62 **B3 17**

eigenvector equation (of a matrix A) The equation $\mathbf{Ax} = k\mathbf{x}$. 62 **B3 17**

element (of a group) A member of the group. 82 **D3 24**

element (of a matrix) See *matrix.*

ellipse A conic having eccentricity between 0 and 1, that is, the set of points P which satisfy $PF = ePd$, where $0 < e < 1$, F is a fixed point (the focus) and d is a fixed line (the directrix) not passing through F. 46 **A2 27**

encipher To apply a cipher. **D2 32**

equal matrices Two matrices are equal if they are of the same size and all their corresponding elements agree. *B2 18*

Equilibrium Condition for forces The relationship between the forces acting on an object at rest. 55 *B3 42*

equilibrium population level The population size at which the proportionate growth rate is zero; that is, the size at which the population remains constant. It is represented by the parameter E in the logistic recurrence relation. 50 *B1 32*

estimated standard error A value used to estimate the standard deviation of a sampling distribution. 78 *D4 22*

Euclid's Algorithm A method for finding the multiplicative inverse, when it exists, of a number in $\mathbb{Z}_n$. 83 **D2 24**

Euler's formula The equation $e^{i\theta} = \cos\theta + i\sin\theta$. **D1 41**

Euler's method A numerical method for solving initial-value problems of the form $dy/dx = f(x, y)$, $y(x_0) = y_0$. 73 *C3 39*

even function A function f with the property that $f(-x) = f(x)$, for all x in the domain of f. **C1 30**

explanatory variable When investigating the relationship between two variables, the variable whose values 'explain' the values taken by the dependent variable. *D4 38*

explicit solution (of a differential equation) A solution written in the form $y = F(x)$, where F is a known function. *C3 15*

exponential form (of a complex number) The complex number with polar form $\langle r, \theta\rangle$ has exponential form $re^{i\theta}$. 79 **D1 43**

exponential function A function with domain $\mathbb{R}$ and rule of the form $f(x) = a^x$ for some positive real number a. The number a is called the base of the exponential function. The most important exponential function is $f(x) = e^x$, where $e = 2.718\,281\ldots$. The function $f(x) = e^x$ is also written as $\exp(x)$. 44 *A3 32*

exponential model (continuous) A model based on a first-order differential equation of the form $dy/dx = Ky$, where K is a constant. Continuous exponential models can be used to model population variation and radioactive decay. 72 *C3 32*

exponential model (discrete) A model for population variation, based on the assumption of a constant proportionate growth rate, r. The model is described by the recurrence relation $P_{n+1} = (1 + r)P_n$, where P_n is the population at n years after some chosen starting time. 50 *B1 22*

factor See *divisor*.

factorial The product of the first n positive integers is called n factorial, and is denoted by $n!$. **B1 42**

fallacious argument A form of argument that is not valid. **D4 17**

Fermat's Little Theorem This theorem states that if p is a prime number and a is a positive integer that is not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$. 83 **D2 27**

Fibonacci numbers The numbers $0, 1, 1, 2, 3, 5, 8, 13, \ldots$, which form the sequence given by 45 **A1 17**

$$F_0 = 0, F_1 = 1,\ F_{n+2} = F_{n+1} + F_n \quad (n = 0, 1, 2, \ldots).$$

finite decimal A number whose decimal representation has a finite number of decimal places. *A0 23*

finite geometric series A sum of the form $a + ar + ar^2 + \cdots + ar^n$. 41 *A1 28*

finite group A group with a finite number of elements (also called a group of finite order). **D3 24**

finite sequence A sequence with a finite number of terms. *A1 6*

first-order differential equation A differential equation that involves the first derivative, dy/dx say, and no higher derivatives. 71 *C3 6*

first-order recurrence relation A recurrence relation in which each term depends on the previous term. *A1 11*

fit value The predicted value of an observation or measurement, based on a model fitted to data. It is the value of the dependent variable which, according to the model, corresponds to a given value of the explanatory variable. 78 *D4 33*

fixed point A number a in the domain of a real function f, such that $f(a) = a$. 56 **B1 14**

fixed point equation The equation $f(x) = x$ for a real function f. 56 **B1 14**

fixed point (of a linear transformation) A point that is equal to its image under the linear transformation. 61 **B3 7**

flattening A linear transformation that maps $\mathbb{R}^2$ onto a line through the origin or onto the origin itself. 59 **B2 30**

floor For a real number x, floor(x) is the greatest integer that is less than or equal to x (also denoted by $[x]$). **D2 8**

focus A point associated with a conic. See also *eccentricity.* 46 **A2 23**

force A push or pull which, if not counteracted, causes the acceleration of an object. *B3 39*

force diagram A diagrammatic representation of the forces acting on an object. *B3 41*

frequency diagram A diagram that represents a data set in which each value (or group of values) is represented by a rectangle whose height is equal to the frequency of that value (or group of values). *D1 35*

frequency (of a particular value, or of an event) The number of times that the value or event occurs. *D2 21*

frieze A plane set whose symmetry group includes non-trivial translations in exactly one direction and which has a translation of shortest displacement. **D3 43**

frieze group The symmetry group of a frieze; it has infinitely many elements. **D3 43**

function A function consists of two sets, called the domain and codomain, and a rule that associates with each x in the domain a unique y in the codomain. A function may also be referred to as a *mapping* or *transformation.* 47 **A3 6**

function of two variables A function whose domain is a subset of $\mathbb{R}^2$ and whose codomain is a subset of $\mathbb{R}$. 47 **A3 12**

general solution (of a differential equation) The set of all possible solutions of the differential equation, usually involving one or more arbitrary constants. 71 *C3 9*

generalised mathematical induction A proof technique that can be used to deduce the truth of a variable proposition $p(n)$ for all natural numbers $n \geq N$, from the knowledge that $p(N)$ is true and that the implication $p(k) \Rightarrow p(k+1)$ is true for all natural numbers $k \geq N$. 88 **D4 38**

generalised scaling A linear transformation represented by a 2×2 matrix that has two distinct non-zero eigenvalues (and hence two distinct eigenlines). 63 **B3 35**

generator See *cyclic group.*

geometric distribution The distribution of the number of trials needed to obtain a success in a sequence of trials of an experiment in which the probability of success in each trial is the same. The probabilities of obtaining the values $1, 2, 3, \ldots$ form a geometric sequence. 75 *D1 39*

geometric form (of a vector) The description of a vector $\mathbf{a}$ in terms of its magnitude $|\mathbf{a}|$ and its direction θ. 54 *B3 11*

geometric mean The geometric mean of a set of n positive numbers is the nth root of the product of the numbers. *A1 19*

geometric sequence A sequence in which each term (apart from the first) is obtained by multiplying the previous term by a fixed number. 40 *A1 19*

geometric series See *finite geometric series* and *infinite geometric series.*

glide-reflection (in a line ℓ) An isometry that is reflection in the line ℓ, followed by a translation parallel to ℓ. 48 **A3 25**

golden ratio The number $\phi = \frac{1}{2}(1 + \sqrt{5}) = 1.618\ldots$. It is the positive solution of the golden ratio equation, $x^2 - x - 1 = 0$. 45 **A1 10**

golden rectangle A rectangle in which the ratio of the length of the longer side to the length of the shorter side is the golden ratio. **A1 10**

gradient (of a graph at a point) The gradient of the tangent to the graph at that point. **B1 19**

gradient (of a line) See *slope (of a line).*

graph (of a real function f) The set of points $(x, f(x))$ in the Cartesian plane. *A3 9*

graphical iteration A geometric construction involving the graphs of $y = f(x)$ and $y = x$, used to determine the long-term behaviour of an iteration sequence generated by the function f. 56 **B1 10**

group A set G and a binary operation on G that satisfy the four conditions of closure, identity, inverses and associativity. 85 **D3 22**

half-life The time that it takes for the mass of a radioactive substance to decay to half of its original amount. 72 *C3 28*

higher derivatives (of a function f) Derivatives $f^{(n)}(x)$ of f, where $n \geq 2$. **C1 16**

histogram A diagram that represents a data set in which each value (or group of values) is represented by a rectangle whose area is proportional to the frequency of that value (or group of values). *D2 15*

horizontal asymptote An asymptote with equation of the form $y = b$. 67 **C1 35**

hyperbola A conic having eccentricity greater than 1, that is, the set of points P which satisfy $PF = ePd$, where $e > 1$, F is a fixed point (the focus) and d is a fixed line (the directrix) not passing through F. 46 **A2 29**

hyperbolic functions Functions such as sinh and cosh. **C3 40**

hypotenuse The longest side of a right-angled triangle. *A2 21*

i-component (of a vector a) The number a_1 in the component form of the vector $\mathbf{a} = a_1\mathbf{i} + a_2\mathbf{j}$. 54 *B3 16*

identity element The element e of a group $(G, *)$, which satisfies $g * e = e * g = g$ for all $g \in G$. 85 **D3 19**

identity matrix A square matrix with all the elements on its leading diagonal equal to 1 and all the other elements equal to 0. 53 *B2 35*

identity transformation The linear transformation which leaves every point of $\mathbb{R}^2$ fixed. It has rule $\mathbf{x} \longmapsto \mathbf{Ix}$, where $\mathbf{I}$ is the identity matrix. 59 **B2 12**

if and only if The operation $\Leftrightarrow$ used to combine propositions. 87 **D4 25**

if ... then The operation $\Rightarrow$ used to combine propositions. 87 **D4 21**

iff An alternative way of writing the operation $\Leftrightarrow$. **D4 25**

image (of x under f) The output of the function f for a given input x, that is, the value of $f(x)$. 47 **A3 6**

image set The complete set of output values of a function. 47 **A3 9**

imaginary part (of a complex number) If $z = a + bi$, then b is the imaginary part of z; it is written as $\mathrm{Im}(z)$. **D1 11**

implication A proposition of the form $p \Rightarrow q$. 87 **D4 21**

implicit differentiation The process of using the Chain Rule to differentiate a function such as $z = H(y)$, where y is a function of x, with respect to x. 71 *C3 16*

implicit solution (of a differential equation) A solution of the form $H(y) = F(x)$, where H and F are known functions, and $H(y) \neq y$. *C3 15*

implies A way of reading the operation $\Rightarrow$. 87 **D4 21**

inclination (of a conic L) The angle θ, where $-\frac{1}{4}\pi < \theta \leq \frac{1}{4}\pi$, through which the conic L must be rotated clockwise about the origin to align its axes of symmetry with the coordinate axes, and so eliminate the cross-term. 49 **A3 44**

increasing function A real function f with the property that for all x_1, x_2 in the domain of f, if $x_1 < x_2$, then $f(x_1) < f(x_2)$. 43 *A3 36*

increasing on an interval A function f is increasing on an interval I if for all x_1, x_2 in I, if $x_1 < x_2$, then $f(x_1) < f(x_2)$. 56 **B1 22**

indefinite integral (of a function $f(x)$ over an interval I) The expression $F(x) + c$, where $F(x)$ is an integral of $f(x)$ over I and c is an arbitrary constant. 67 **C2 6**

independent events Two events are independent if the occurrence (or not) of one event is not influenced by whether or not the other occurs. 75 *D1 29*

independent variable A variable that can take on any value appropriate to the problem; that is, its value does not depend on the value of any other variable. *A0 28*

indifferent 2-cycle A 2-cycle a, b of a smooth function f for which $|f'(a)f'(b)| = 1$. 57 **B1 36**

indifferent fixed point A fixed point a of a smooth function f for which $|f'(a)| = 1$. 56 **B1 25**

infinite decimal A number whose decimal representation has infinitely many decimal places. *A0 23*

infinite geometric series A sum of the form $a + ar + ar^2 + \cdots$. 50 *B1 48*

infinite group A group with infinitely many elements; it is also called a group of infinite order. **D3 24**

infinite sequence A sequence that has a first term but no final term. *A1 6*

initial condition (for a first-order differential equation) A condition requiring that the dependent variable take a specified value when the independent variable has a given value. 71 *C3 10*

initial-value problem The combination of a first-order differential equation and an initial condition. 71 *C3 10*

integers The positive and negative whole numbers, together with zero: $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$. *A0 23*

integral (of a function $f(x)$ over an interval I) A function $F(x)$ for which $F'(x) = f(x)$ for all $x \in I$, where I is an interval in the domains of F and f. 67 **C2 6**

integrand In an integral, the function which is to be integrated. 67 *C2 8*

integration The process of finding either an integral or the indefinite integral of a function. 67 *C2 8*

integration by parts A method of transforming an integral of a function of the form $f(x)g'(x)$ into a different integral that may be more easily evaluated. 70 **C2 24**

integration by substitution A method of transforming an integral of a function, typically of the form $f(g(x))g'(x)$, into a different integral that may be more easily evaluated. 70 **C2 33**

intercept A value of x or y where a line (or curve) meets the x-axis or y-axis, respectively. 43 *A2 11*

interquartile range The difference between the upper quartile and the lower quartile of a batch of data. 77 *D4 11*

interval An unbroken subset of the real line. *A3 7*

interval of attraction An open interval I, containing an attracting fixed point a, with the property that if x_0 is in I and x_n is generated by iteration of f, then $x_n \to a$ as $n \to \infty$. 57 **B1 25**

invariant line (of a linear transformation) A line that is equal to its image under the linear transformation. 61 **B3 9**

inverse element In a set S with operation $\circ$, the inverse element a^{-1} of a (where it exists) satisfies $a \circ a^{-1} = e = a^{-1} \circ a$, where e is the identity element. 85 **D3 22**

inverse function The inverse function (or inverse) f^{-1} of a one-one function f reverses the effect of f; that is, if $f(x) = y$, then $f^{-1}(y) = x$. The domain of f^{-1} is the image set of f. 43 *A3 37*

inverse (of a matrix) If two square matrices $\mathbf{A}$ and $\mathbf{B}$ have the property that $\mathbf{AB} = \mathbf{BA} = \mathbf{I}$, where $\mathbf{I}$ is the identity matrix, then each of $\mathbf{A}$ and $\mathbf{B}$ is the inverse of the other. 53 *B2 36*

inverse symmetry For a symmetry f in $S(X)$, the inverse symmetry f^{-1} in $S(X)$ has the property that $f \circ f^{-1} = e = f^{-1} \circ f$. 85 **D3 20**

invertible linear transformation A linear transformation that is represented by an invertible matrix $\mathbf{A}$. 60 **B2 42**

invertible matrix A square matrix that has a non-zero determinant, and therefore has an inverse. 53 *B2 38*

irrational number A real number that is not rational, and hence is a non-recurring decimal. *A0 24*

isometry (of the plane) A function with domain and codomain $\mathbb{R}^2$, which preserves the distances between points. Every isometry is one of four basic types: a translation, a rotation, a reflection or a glide-reflection. 48 **A3 15**

isomorphism (of groups) Two finite groups are isomorphic if there is a one-one function from one group onto the other, which converts a Cayley table of the first group to a Cayley table of the second group. 86 **D3 33**

iteration The repeated application of a function or process. **B1 4**

iteration sequence A sequence x_n obtained by iterating a (real) function f using the recurrence relation $x_{n+1} = f(x_n)$ $(n = 0, 1, 2, \ldots)$ with initial term x_0. **B1 9**

iteration sequence (generated by a matrix A) A sequence of points represented by the vectors $\mathbf{x}_n$, obtained by applying the recurrence relation $\mathbf{x}_{n+1} = \mathbf{A}\mathbf{x}_n$ $(n = 0, 1, 2, \ldots)$ with initial point represented by the vector $\mathbf{x}_0$. 63 **B3 39**

j-component (of a vector a) The number a_2 in the component form of the vector $\mathbf{a} = a_1\mathbf{i} + a_2\mathbf{j}$. 54 *B3 16*

key A parameter in a family of ciphers. **D2 33**

leading coefficient (of a polynomial) In the polynomial function $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $n \geq 1$ and $a_n \neq 0$, we call a_n the leading coefficient. **C1 34**

leading diagonal (of a matrix) The diagonal of a square matrix which starts at the top left and ends at the bottom right of the matrix. *B2 36*

least squares A method for fitting a line or curve to a set of data points in such a way that the sum of the squared residuals is as small as possible. 78 *D4 34*

least squares fit line The straight line that is fitted using the method of least squares. 78 *D4 35*

left-skew See *skewed.*

lemma A minor result, usually preparing the way for a theorem. **D2 6**

limit (of a sequence) The value near which a convergent sequence settles in the long term. 51 *B1 42*

limits of integration The numbers a and b in the expression $\int_a^b f(x)\,dx$. The number a is the lower limit and b is the upper limit. 67 *C2 41*

linear expression A sum consisting of first powers of the variables and a constant. *A0 35*

linear function A real function with rule of the form $f(x) = mx + c$ for some constants m and c. *A3 9*

linear recurrence sequence A recurrence sequence with recurrence relation of the form $x_{n+1} = rx_n + d$, where r and d are constants. 40 *A1 24*

linear second-order recurrence sequence A recurrence sequence with recurrence relation of the form $u_{n+2} = pu_{n+1} + qu_n$, where p and q are constants. 45 **A1 23**

linear transformation A function with domain and codomain $\mathbb{R}^2$, and rule of the form $\mathbf{x} \longmapsto \mathbf{Ax}$, where $\mathbf{A}$ is a 2×2 matrix. The linear transformation is said to be represented by the matrix $\mathbf{A}$. 59 **B2 16**

local maximum A function f has a local maximum at x_0, with value $f(x_0)$, if $f(x_0)$ is the greatest function value in the immediate vicinity of x_0. 66 **C1 32**

local minimum A function f has a local minimum at x_0, with value $f(x_0)$, if $f(x_0)$ is the least function value in the immediate vicinity of x_0. 66 **C1 32**

locus A curve defined by a particular property. *A2 7*

logarithm to the base a The inverse function of the exponential function $f(x) = a^x$, where $a > 0$ and $a \neq 1$. The logarithm function is written $\log_a$ and has domain $(0, \infty)$. 44 *A3 42*

logistic model A model for population variation, based on the assumption of a proportionate growth rate of the form $R(P) = r(1 - P/E)$, where r and E are positive parameters. 50 *B1 29*

logistic recurrence relation A recurrence relation of the form $P_{n+1} - P_n = rP_n(1 - P_n/E)$, where r and E are positive parameters. 50 *B1 29*

log-linear plot A plot of the natural logarithm of the dependent variable against the independent variable. 72 *C3 33*

long-term behaviour of a sequence The way in which the sequence develops as more and more terms are considered. 40 *A1 32*

lower quartile See *quartiles.*

Lucas numbers The numbers $2, 1, 3, 4, 7, 11, 18, 29, \ldots$, which form the sequence given by **A1 29**

$$L_0 = 2, L_1 = 1,\ L_{n+2} = L_{n+1} + L_n \quad (n = 0, 1, 2, \ldots).$$

Maclaurin polynomial A Taylor polynomial about 0. **C3 34**

Maclaurin series A Taylor series about 0. **C3 34**

magnitude (of a real number) See *modulus (of a real number x).*

magnitude (of a vector a) The length of an arrow representing the vector; it is written as $|\mathbf{a}|$. 54 *B3 10*

main diagonal (of a matrix) See *leading diagonal (of a matrix).*

major axis (of an ellipse) The line segment from $(-a, 0)$ to $(a, 0)$ for the ellipse $x^2/a^2 + y^2/b^2 = 1$, where $a \geq b > 0$. **A2 14**

many-one function A function that is not one-one. **B2 31**

mapping See *function.*

mass A measure of the amount of matter that an object contains. *B3 40*

mathematical induction A proof technique that can be used to deduce the truth of a variable proposition $p(n)$ for all natural numbers n, from the knowledge that $p(1)$ is true and that the implication $p(k) \Rightarrow p(k+1)$ is true for all natural numbers k. 88 **D4 30**

mathematical model A collection of formulas that attempts to quantify how some aspect of the real world behaves. 4 *A1 36*

matrix A rectangular array of numbers. Each number in a matrix is called an element of the matrix. A row of the matrix is a horizontal line of numbers in the array, and a column of the matrix is a vertical line of numbers in the array. A matrix with m rows and n columns is called an $m \times n$ matrix. Matrices of appropriate sizes can be added, subtracted and multiplied. 52 *B2 11*

matrix–vector multiplication The process of multiplying a vector by a matrix. 52 *B2 13*

mean An average of a finite set of numbers. See *arithmetic mean, geometric mean.*

mean (of a probability distribution, or of a random variable) The average value predicted by the probability model. 75 *D1 43*

median If the values in a batch of data are written in order of increasing size, then the median is the middle value when the batch size is odd, or the average of the middle two values when the batch size is even. 77 *D4 8*

messagetext (message) A messagetext (to be enciphered) is a finite sequence of characters chosen from a finite set. 83 **D2 32**

minor axis (of an ellipse) The line segment from $(0, -b)$ to $(0, b)$ for the ellipse $x^2/a^2 + y^2/b^2 = 1$, where $a \geq b > 0$. **A2 14**

mode A peak in a distribution. A distribution that has only one peak is called unimodal; a distribution that has two peaks is called bimodal. *D2 9*

modelling cycle The process of choosing a (mathematical) model, trying it out, evaluating it, and possibly changing it. 4 *A1 37*

modular arithmetic Arithmetic performed in $\mathbb{Z}_n$. 82 **D2 21**

modulus (of a complex number) If $z = a + bi$, then $\sqrt{a^2 + b^2}$ is the modulus of z; it is written as $|z|$. 79 **D1 26**

modulus (of a congruence) In the congruence $a \equiv b \pmod{n}$, n is the modulus. 81 **D2 9**

modulus (of a real number x) The magnitude of x, regardless of its sign; it is written as $|x|$. 42 *A3 13*

Modus Ponens A general form of deduction in which the propositions p and $p \Rightarrow q$ are known to be true, and it is deduced that q is true. 88 **D4 27**

multiplicative inverse If a and b are positive integers in $\mathbb{Z}_n$ and $a \times_n b = 1$, then b is the multiplicative inverse of a in $\mathbb{Z}_n$. 82 **D2 24**

natural logarithm The logarithm function with base e, where $e = 2.718\,281\ldots$; it is often written as ln. 44 *A3 45*

natural numbers The positive integers: $1, 2, 3, \ldots$. *A0 23*

necessary condition If $q \Rightarrow p$ is true, then p is a necessary condition in order that q holds. **D4 25**

negative on an interval A function f is negative on an interval I if $f(x) < 0$, for all $x \in I$. **C1 31**

network diagram A mathematical representation of a physical network. Each point at which a network branches is called a node, and two nodes of a network may be connected by a pipe. 51 *B2 6*

newton The SI unit of force. *B3 40*

Newton–Raphson method An interation method for finding an approximate solution of the equation $f(x) = 0$. 67 **C1 43**

n-gon A regular polygon with n sides. **D3 13**

node (of a network) See *network diagram.*

non-invertible matrix A square matrix that has zero determinant, and therefore has no inverse. 53 *B2 38*

normal curve The graph of the probability density function of a normal distribution. 76 *D2 13*

normal distribution A particular model for the variation in a continuous random variable. 76 *D2 13*

normal reaction The force acting on an object due to contact with a surface, which is directed at right angles to that surface. *B3 41*

nth derivative (of a function f at a point x) The value of the nth derived function of f at the point x, denoted by $f^{(n)}(x)$. **C1 16**

nth derived function (of a function f) The function $f^{(n)}$ defined by the process of differentiating n times the function f. **C1 16**

nth root of a The non-negative number which, when raised to the power n, gives the answer a. 37 *A0 26*

nth root of unity A complex number z such that $z^n = 1$. 80 **D1 36**

n-times-differentiable function A function that can be differentiated n times at each point of its domain. **C1 16**

null hypothesis A hypothesis H_0 about a population (or populations) which may or may not be rejected as the result of a hypothesis test. 78 *D4 18*

odd function A function f with the property that $f(-x) = -f(x)$, for all x in the domain of f. **C1 30**

one-one function A function $f : A \longrightarrow B$ with the property that each element of $f(A)$ is the image of exactly one element of A; that is, for all $a, b \in A$, if $a \neq b$, then $f(a) \neq f(b)$. 60 **B2 31**

onto function A function $f : A \longrightarrow B$ such that $f(A) = B$. 60 **B2 32**

optimisation The process of finding optimum values of a function on an interval. 66 *C1 32*

optimum values (on an interval) The greatest or least values attained by a function on the interval. 66 *C1 32*

or The operation $\vee$ used to combine propositions. 87 **D4 22**

order (of a differential equation) The order of the highest derivative that appears in the differential equation. *C3 6*

order (of a group) The number of elements in the group. 85 **D3 24**

parabola A conic having eccentricity 1, that is, the set of points P which satisfy $PF = ePd$, where $e = 1$, F is a fixed point (the focus) and d is a fixed line (the directrix) not passing through F. 46 **A2 23**

Parallelogram Rule A rule for the addition of two vectors that are in geometric form. 54 *B3 14*

parameter (1) A variable used when defining a family of mathematical objects, such as a recurrence system. 40 *A1 14*

parameter (2) A variable, often t, used when defining a curve in terms of the motion of a point along the curve. 42 *A2 40*

parametrisation function (for a curve) A function whose domain is an interval of $\mathbb{R}$ and whose image set is the curve. **A3 10**

parametrisation (of a curve) The process of describing the coordinates of points on the curve in terms of a parameter. 42 *A2 40*

particle A material object whose size and internal structure may be neglected (for modelling purposes). *B3 40*

particular solution (of a differential equation) A single solution of the differential equation, which contains no arbitrary constant. 71 *C3 9*

Pascal's triangle The triangle of numbers used to generate binomial coefficients. **B1 40**

p-cycle Distinct numbers $a_1, a_2, \ldots, a_p$ in the domain of a real function f such that $f(a_1) = a_2$, $f(a_2) = a_3$, $\ldots$, $f(a_p) = a_1$. 58 **B1 39**

periodic function A function f whose graph is unchanged by a horizontal translation through the period p; that is, $f(x + p) = f(x)$ for all x in the domain. *A3 28*

permutation An arrangement of objects (all different) in a particular order. 58 **B1 42**

permutation (of n objects taken k at a time) An arrangement formed by choosing k objects from n objects (all different) and placing them in a particular order. 58 **B1 43**

perpendicular bisector (of a line segment AB) The line that cuts AB halfway along its length and is at right angles to AB. *A2 24*

pipe (of a network) See *network diagram.*

plane set A subset of $\mathbb{R}^2$. **D3 6**

polar coordinates (of a point A) The numbers r and θ for the point A with Cartesian coordinates $(r\cos\theta, r\sin\theta)$. *B3 19*

polar form (of a complex number) The representation of a complex number in the form $\langle r, \theta \rangle$, where r is its distance from 0 and θ is its angle measured anticlockwise from the x-axis (on an Argand diagram). 79 **D1 25**

polygonal approximation (to a function F) An approximation to the graph of F by a graph consisting of line segments joined end to end. **C2 21**

polynomial A polynomial (of degree n) is an expression of the form $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_n \neq 0$. *A3 47*

polynomial function A function whose rule is a polynomial; for example, a quadratic function. *A3 47*

population The collection of all the individual values or members of a specified group of interest. *D2 8*

population mean The mean of all the values in a population or, when a probability distribution is used to model the variation in the population, the mean of this probability distribution. 76 *D2 23*

population parameter A summary measure for a population. The population mean μ and the population standard deviation σ are examples of population parameters. 76 *D2 20*

population standard deviation The square root of the population variance. 76 *D2 24*

population variance The mean squared deviation of the values in a population from the population mean. *D2 24*

position The position of a particle, with respect to a chosen axis, is a measure of how far it is from the origin and of its direction relative to the origin. 69 *C2 26*

position vector The vector representation of a point in the plane. For example, the point $P(x, y)$ has position vector $\overrightarrow{OP} = \mathbf{p} = \begin{pmatrix} x \\ y \end{pmatrix}$. 59 **B2 9**

positive on an interval A function f is positive on an interval I if $f(x) > 0$, for all $x \in I$. **C1 31**

power function A function with rule of the form $f(x) = x^n$, where n is any real number. *C1 16*

power (of a square matrix) The nth power of a square matrix $\mathbf{A}$, written $\mathbf{A}^n$, is obtained by repeated matrix multiplication. 52 *B2 21*

predicted value See *fit value.*

premise In a deductive argument, a premise is a statement whose truth is known at the outset of the argument. **D4 16**

principal value (of $\arg(z)$) The unique value of $\arg(z)$ that lies in the interval $(-\pi, \pi]$. 79 **D1 28**

probability density function If a curve is used to model the variation in a population, and the total area between the curve and the x-axis is 1, then the function that defines the curve is a probability density function. According to the model, the proportion of the population between two values a and b $(a < b)$ is given by the area under the curve between $x = a$ and $x = b$. 75 *D2 13*

probability distribution The probability distribution of a random variable gives the probabilities of all the possible values that the random variable can take. 75 *D1 38*

probability function The probability function of a discrete random variable X is a function that gives, for each value j, the value of the probability $P(X = j)$. 75 *D1 37*

probability (of an event) The long-run proportion of occasions on which the event occurs. 75 *D1 10*

product matrix The result of multiplying two matrices together. *B2 16*

proof by contradiction A method of proof in which the desired conclusion is assumed to be false, and a contradiction is then deduced. **D4 12**

proof by exhaustion A method of proof in which each of a finite number of possible cases is checked individually. **D4 13**

proportionate growth rate The proportionate birth rate minus the proportionate death rate for a population. *B1 22*

proportionate growth rate (continuous exponential model) The constant K in the differential equation $dP/dt = KP$, used to model population variation. 72 *C3 31*

proposition A statement, which must be either true or false. 87 **D4 19**

***p*th iterate of f** The composite function $f \circ f \circ \ldots \circ f$, denoted f^p, obtained when the function f is applied p times. 58 **B1 39**

quadratic curve A curve represented by an equation of the form $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$, where A, B, C are not all zero. 47 **A2 34**

quadratic expression An expression of the form $ax^2 + bx + c$, where $a \neq 0$. *A0 37*

quartic function A polynomial function of degree 4. *C1 20*

quartiles The median and quartiles of a batch of data divide the batch into four roughly equal parts. Roughly 25% of the values in a batch are smaller than the lower quartile, and roughly 25% of the values are greater than the upper quartile. When the values are written in order of increasing size, the lower quartile is the median of the values to the left of the median, and the upper quartile is the median of the values to the right of the median. 77 *D4 8*

quotient If a, n, q and r are integers with $n > 0$, and $a = qn + r$ with $0 \leq r < n$, then q is the quotient on division of a by n. 81 **D2 7**

radius (of a circle) The distance from the centre of the circle to any point on the circumference of the circle. *A2 20*

random variable A quantity that can take different values on different occasions. *D1 36*

range The range of a batch of data is the difference between the maximum and minimum values. 77 *D4 11*

range of validity A range of values of x for which the Taylor series (in x) for a function f sums to $f(x)$. 73 **C3 30**

rational function A function with rule of the form $f(x) = p(x)/q(x)$, where both p and q are polynomial functions. 67 **C1 34**

rational number A real number that can be represented as a fraction, and hence as a recurring decimal. *A0 23*

rationalising the denominator The process of rearranging a fraction with square root signs in the denominator as an equivalent fraction without square root signs in the denominator. 45 **A1 11**

real function A function for which both the inputs and the outputs are real numbers. *A3 9*

real line A number line that includes all real numbers. *A0 24*

real number A number that can be represented as a decimal. *A0 23*

real part (of a complex number) If $z = a + bi$, then a is the real part of z; it is written as $\mathrm{Re}(z)$. **D1 11**

reciprocal function The function whose rule is $f(x) = 1/x$. *A3 10*

reciprocal (of a complex number) The reciprocal of z is $1/z$. 79 **D1 18**

rectangular hyperbola A hyperbola for which the asymptotes are at right angles. **A2 17**

recurrence relation A formula that defines each term of a sequence by referring to a previous term or terms of the sequence. 40 *A1 11*

recurrence system The specification of a sequence by an initial term or terms, a recurrence relation and a subscript range. 40 *A1 11*

reflected standard position A conic is in reflected standard position if it can be obtained from a conic in standard position by exchanging the roles of x and y. 49 **A3 42**

reflection (in a line ℓ) A function that maps each point P of the plane to a point P' on the other side of ℓ in such a way that ℓ is the perpendicular bisector of the line segment PP', with the points on ℓ kept fixed. 48 **A3 23**

regression line The regression line of y on x is another name for the least squares fit line. See also *least squares fit line.* 78 *D4 35*

remainder If a, n, q and r are integers with $n > 0$, and $a = qn + r$ with $0 \leq r < n$, then r is the remainder on division of a by n. 81 **D2 7**

remainder function The function r with rule $r(x) = f(x) - p(x)$, where f is a function and p is a polynomial that is intended to approximate f. **C3 7**

repeated root (of a polynomial $p(z)$) A number α such that $(z - \alpha)^2$ is a factor of $p(z)$. 80 **D1 34**

repelling 2-cycle A 2-cycle a, b of a smooth function f for which $|f'(a)f'(b)| > 1$. 57 **B1 36**

repelling fixed point A fixed point a of a smooth function f for which $|f'(a)| > 1$. 56 **B1 24**

residual When a line is fitted to a set of data points, the residual of each data pair may be calculated using the relationship RESIDUAL = DATA − FIT, where DATA is the y-coordinate of the data pair and FIT is the y-value predicted by the line for the corresponding x-coordinate. 78 *D4 33*

resultant The sum of two vectors. *B3 13*

right circular cone A cone for which the cross-sections obtained by slicing the cone with planes at right angles to the axis are circles. **A2 8**

right-skew See *skewed.*

rise from A to B The rise from a point $A(x_1, y_1)$ to a point $B(x_2, y_2)$ is $y_2 - y_1$. *A2 9*

root (of a polynomial $p(z)$) A solution of the equation $p(z) = 0$. 80 **D1 32**

rotation (of the plane) A function that moves each point of the plane through a fixed angle about a fixed point. 48 **A3 19**

row (of a matrix) See *matrix.*

rule (of a function) The process for converting each input value in the domain of the function into a unique output value. See also *function.* 47 **A3 6**

run from A to B The run from a point $A(x_1, y_1)$ to a point $B(x_2, y_2)$ is $x_2 - x_1$. *A2 9*

sample A subset of a population. 76 *D2 8*

sample mean The mean $\overline{x}$ of a sample. 76 *D2 21*

sample standard deviation The sample standard deviation s is the square root of the sample variance. 76 *D2 25*

sample variance The mean squared deviation, from the sample mean, of the values in a sample. *D2 25*

sampling distribution of the mean The distribution of the means of all possible samples of size n from a population is called the sampling distribution of the mean for samples of size n. 77 *D3 10*

sampling error An error due to the selection of an unrepresentative sample. *D3 30*

scalar A real number. *B2 23*

scalar multiplication (of a matrix) The operation of multiplying each element of a matrix $\mathbf{A}$ by a real number k. The resulting matrix $k\mathbf{A}$ is called the scalar multiple of $\mathbf{A}$ by the real number k. 52 *B2 23*

scaling (of a graph) Squashing or stretching the graph in the x-direction or y-direction. 43 *A3 21*

scaling (with factors a and b) A linear transformation represented by the matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, where $a \neq 0$ and $b \neq 0$. 59 **B2 23**

secant (of an angle θ) The secant of θ is $1/\cos\theta$, provided that $\cos\theta \neq 0$. *A2 36*

second derivative (of a function f at a point) The value of the second derived function f'' at the point. 66 *C1 28*

second derived function (of a function f) The function f'' defined by the process of differentiating the derived function f' of f. 66 *C1 28*

second-order recurrence relation A recurrence relation in which each term depends on the previous two terms. 45 **A1 17**

self-inverse (element of a group) An element g of a group $(G, *)$ such that $g^{-1} = g$ (or, equivalently, $g * g = e$). 85 **D3 20**

separable differential equation A differential equation of the form $dy/dx = f(x)g(y)$. 72 *C3 19*

separation of variables A method for solving separable differential equations. 72 *C3 19*

sequence An ordered list (finite or infinite) of numbers, called the terms of the sequence. 40 *A1 6*

series A sum of consecutive terms of a sequence. 50 *B1 11*

set A collection of objects (without regard to their order, and without repetitions).

shear (parallel to a line ℓ) A linear transformation that shifts each point P parallel to ℓ, through a distance that is proportional to the perpendicular distance of P from ℓ. 59 **B2 25**

sigma notation A concise way of expressing finite and infinite series. 50 *B1 11*

signed area A value for area in which regions above the x-axis are regarded as having positive areas and regions below the x-axis are regarded as having negative areas. **C2 18**

significance level The significance level of a test is the probability (often written as a percentage) that the null hypothesis is wrongly rejected. 78 *D4 23*

sine (of an angle θ) The second coordinate of the point P on the circumference of the unit circle, centre O, where the angle between the positive x-axis and the line segment OP is θ. By convention, angles are measured positively in an anticlockwise direction from the positive x-axis. 41 *A2 33*

Sine Rule A rule that relates pairs of sides and the corresponding opposite angles of a triangle. 55 *B3 31*

sinh x The hyperbolic sine function. 74 **C3 40**

size (of a matrix) An $m \times n$ matrix has size $m \times n$. 52 *B2 18*

skewed A data set which is not symmetric (or, equivalently, for which a frequency diagram is not symmetric) is said to be skewed. If the large data values are more spread out than the small data values, so that a frequency diagram has a longer right tail than left tail, then the data set is right-skew. If the left tail of a frequency diagram is longer than the right tail, then the data set is left-skew. The terms right-skew and left-skew are also used to describe probability distributions. *D2 11*

slope (of a line) If A and B are two points on a line, then the slope of the line is (rise from A to B) $\div$ (run from A to B). The slope is also called the gradient. 41 *A2 9*

smooth function Informally, a function is smooth if there is a tangent at each point of its graph. **B1 19**

solid of revolution A solid constructed by rotating a region bounded by the graph of a continuous function f, the x-axis and the lines $x = a$ and $x = b$ through 360° about the x-axis. 70 **C2 42**

solution of a differential equation A function, $y = F(x)$ say, (or a more general equation relating the independent and dependent variables) for which the differential equation is satisfied. 71 *C3 6*

solving a triangle The process of determining all the angles and side lengths of a triangle. *A2 37*

speed A (scalar) measure of how fast an object is moving, irrespective of its direction of motion. The speed is the magnitude of the velocity vector. *B3 26*

square matrix A matrix with the same number of rows and columns. *B2 21*

standard error The standard deviation of a sampling distribution. *D3 14*
D4 20

standard error of the mean The standard deviation of the sampling distribution of the mean for samples of size n, for any given sample size n. 77 *D3 14*

standard normal distribution The normal distribution with mean 0 and standard deviation 1. 76 *D2 36*

star polygon A figure obtained by placing n points evenly around a circle and joining successive pairs of points that are a points apart, where $1 < a < n - 1$. **D2 26**

stationary point A point x_0 in the domain of a smooth function f at which $f'(x_0) = 0$, or the corresponding point $(x_0, f(x_0))$ on the graph of f. 66 *C1 22*

step size The value of the variable h in Euler's method, which determines the distance between the successive values of x at which solution estimates are calculated. 73 *C3 39*

subgroup If $(G, *)$ is a group and H is a subset of G, then H is a subgroup of G if $(H, *)$ forms a group; that is, the operation $*$ is closed on H, the identity element of G is in H and, if a is in H, then its inverse a^{-1} is also in H. **D3 29**

subscript In the notation a_n, n is called the subscript of a. *A1 7*

subset The set A is a subset of the set X if each element of A is also an element of X. **A3 9**

subtended angle (at a point) The angle that lies between two lines drawn from the point to the endpoints of a line segment or an arc of a circle. *A2 21*

sufficient condition If $p \Rightarrow q$ is true, then p is a sufficient condition in order that q holds. **D4 25**

super-attracting 2-cycle A 2-cycle a, b of a smooth function f for which $f'(a)f'(b) = 0$. 57 **B1 36**

super-attracting fixed point A fixed point a of a smooth function f for which $f'(a) = 0$. 56 **B1 25**

surface plot The graph of a function f of two variables, that is, the set of points (x, y, z) in three-dimensional space satisfying $z = f(x, y)$. 47 **A3 13**

symmetry group The group consisting of all the symmetries of a given plane set. 85 **D3 22**

symmetry (of a plane set) A (plane) isometry that maps the plane set to itself. 85 **D3 7**

tangent (of an angle θ) $\tan\theta = \dfrac{\sin\theta}{\cos\theta}$, where $\theta \neq \pm\frac{1}{2}\pi, \pm\frac{3}{2}\pi, \ldots$. 41 *A2 36*

tangent (to a circle) A line that intersects the circle in precisely one point. *A2 29*

tangent (to a graph) The unique line through a point on the graph, that just 'touches' the graph at that point. **B1 19**

Taylor polynomial of degree n A polynomial of degree at most n which approximates a given function near a given point; Taylor polynomials of degree at most $0, 1, 2, 3, 4, 5$ are called constant, linear, quadratic, cubic, quartic, quintic Taylor polynomials, respectively. 73 **C3 17**

Taylor series The infinite series obtained by letting the degree of a Taylor polynomial tend to infinity. 73 **C3 30**

telescoping cancellation A form of simplification that involves repeated cancelling when adding expressions. **A1 32**

tends to infinity (or minus infinity) The terms of a sequence become arbitrarily large and positive (or arbitrarily large and negative). *A1 33*

tends to ℓ The terms of a sequence become arbitrarily close to ℓ. *A1 33*

tension The force provided by a taut string (rope, etc.). *B3 41*

term (of a sequence) An item of a sequence. 40 *A1 6*

test statistic A measure calculated from data, which can be used to decide whether or not to reject the null hypothesis. 78 *D4 22*

theorem A key result or list of key results. **D2 6**

trace The sum of the diagonal entries of a square matrix. **B3 19**

transformation An alternative name for a function in a geometrical context. See also *function*.

translation A function that moves each point of the plane a fixed distance in a fixed direction. 48 **A3 8**

translation (of a graph) Shifting the graph horizontally or vertically. 43 *A3 20*

triangle of forces A triangle of arrows which is a geometric representation of the Equilibrium Condition for three forces. *B3 44*

Triangle Rule A rule for the addition of two vectors that are in geometric form. 54 *B3 13*

triangular matrix A square matrix with either all the elements above the leading diagonal equal to zero or all the elements below the leading diagonal equal to zero. **B2 41**

truth table A table showing the truth value of a compound proposition for all possible combinations of the propositions that are combined. 87 **D4 21**

truth value The truth or falsity of a proposition. 87 **D4 21**

two-cycle Distinct numbers a and b in the domain of a real function f such that $f(a) = b$ and $f(b) = a$. 57 **B1 34**

two-cycle equation The equation $f(f(x)) = x$ for a real function f. 57 **B1 34**

unbounded figure A figure that does not lie within any circle. **A2 15**

unbounded sequence A sequence that has terms of arbitrarily large value, either positive or negative. 40 *A1 34*

unbounded set See *bounded set.*

uniform scaling (with factor a) A linear transformation represented by a matrix of the form $a\mathbf{I}$, where $a \neq 0$ and $\mathbf{I}$ is the identity matrix. 59 **B2 24**

unimodal See *mode.*

union (of sets A and B) The set consisting of all elements of both A and B. **D3 29**

unit circle The circle with radius 1 and centre at the origin. *A2 33*

unit grid The grid in $\mathbb{R}^2$ of horizontal and vertical lines passing through all points of the form (m, n), where $m, n \in \mathbb{Z}$. **B2 19**

unit square The square in $\mathbb{R}^2$ with vertices at $(0, 0)$, $(1, 0)$, $(1, 1)$ and $(0, 1)$. **B2 12**

upper quartile See *quartiles.*

variable A symbol used to represent a quantity that can vary. *A0 28*

variable proposition A proposition involving a variable from a specified set; its truth value depends on the value of the variable. 87 **D4 23**

vector A matrix consisting of a single column. Each number appearing in the column is called a component of the vector. 53 *B2 10*

velocity (vector) The rate of change of position of an object. Velocity is a measure of how fast the object is moving and its direction of motion. *B3 26*

vertex (of a conic) A point where the conic meets an axis of symmetry of the conic (a line in which the conic is symmetric). **A2 14**

vertex (of a double cone) The point at which the two cones meet. This point is also called the apex of the cone. **A2 8**

vertical asymptote An asymptote with equation of the form $x = a$. 67 **C1 35**

wallpaper A plane set whose symmetry group includes non-trivial translations in at least two non-parallel directions and which has a translation of shortest displacement. **D3 43**

wallpaper group The symmetry group of a wallpaper; it has infinitely many elements. **D3 43**

weight The force on an object due to gravity. *B3 40*

x-shear (with factor a) A shear parallel to the x-axis, represented by the matrix $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, where $a \in \mathbb{R}$. 59 **B2 25**

y-shear (with factor a) A shear parallel to the y-axis, represented by the matrix $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, where $a \in \mathbb{R}$. 59 **B2 25**

zero (of a function f) A solution of the equation $f(x) = 0$, also referred to as an x-intercept of f. **C1 31**

zero transformation The linear transformation represented by the 2×2 matrix whose elements are all 0. **B2 29**

zero vector The vector in which every component is 0, denoted by $\mathbf{0}$. *B3 8*

Background material for MST121 and MS221

Rounding numbers

To **round** to a given number of **decimal places**, look at the digit one place to the right of the number of places specified. If this digit is 5 or more, then round up; if it is less than 5, then round down.

To **round** to a given number of **significant figures**, start counting significant figures from the first non-zero digit on the left, and follow the rules for rounding.

Scientific notation

In scientific notation, positive numbers are expressed in the form $a \times 10^n$, where a is between 1 and 10, and n is an integer.

Rules for powers

$a^p \times a^q = a^{p+q}$ $\quad a^p \div a^q = a^{p-q}$ $\quad (a^p)^q = a^{pq}$ $\quad a^p b^p = (ab)^p$

$a^{-n} = \dfrac{1}{a^n}$ $\quad a^0 = 1$ $\quad a^{1/n} = \sqrt[n]{a}$ $\quad a^{m/n} = (\sqrt[n]{a})^m = \sqrt[n]{a^m}$

Calculating means

To calculate the **mean** of a batch of data, add together the values (x) in the batch to give $\sum x$, and divide by n, the number of values in the batch.

Algebra

Difference of two squares: $a^2 - b^2 = (a - b)(a + b)$.

Squaring a bracket: $(a + b)^2 = a^2 + 2ab + b^2$.

The **solutions of the quadratic equation** $ax^2 + bx + c = 0$, where $a \neq 0$, are

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

To solve two simultaneous linear equations by **substitution**.

1. Rearrange one of the equations so that one unknown is equal to an expression involving the other unknown.
2. Substitute this expression in the other equation.
3. Solve the resulting linear equation for the other unknown.
4. Substitute this solution into either of the original equations to find the remaining unknown.

To solve two simultaneous linear equations by **elimination**.

1. Multiply the two equations by numbers chosen so that one of the unknowns has the same coefficient, possibly with the opposite sign, in both equations.
2. Subtract or add the new equations to eliminate that unknown.
3. Solve the resulting linear equation for the other unknown.
4. Substitute this solution into either of the original equations to find the remaining unknown.

Equivalent rearrangements of inequalities

If the sides of an inequality are interchanged, then the direction of the inequality sign is reversed: $>$ becomes $<$, $\geq$ becomes $\leq$, and vice versa.

The same number can be added to (or subtracted from) both sides of an inequality: if $a < b$, then $a + c < b + c$.

Both sides of an inequality can be multiplied (or divided) by the same positive number: if $a < b$ and $c > 0$, then $ac < bc$.

If both sides of an inequality are multiplied (or divided) by the same negative number, then the direction of the inequality sign changes: if $a < b$ and $c < 0$, then $ac > bc$.

Angle measurement

The angle subtended at the centre of a circle by an arc equal in length to the radius of the circle is defined to be one **radian**. Thus 2π radians $= 360°$, and the rules for converting between degrees and radians are

$$x \text{ radians} = x \times \frac{180}{\pi} \text{ degrees}, \quad y \text{ degrees} = y \times \frac{\pi}{180} \text{ radians}.$$

Polygons

A plane figure which is a closed shape whose sides are straight lines is called a **polygon**. A point where two sides meet is called a **vertex**. A polygon with n sides (and hence n vertices) is referred to as an ***n*-gon**.

The angle sum of an n-gon is $(n-2)180°$, that is, $(n-2)\pi$ radians.

An n-gon is said to be **regular** if all its sides are equal and all its angles are equal.

Triangles

A **triangle** is a polygon with three sides. Its angle sum is $180°$, that is, π radians. If all three sides are of equal length, then it is an **equilateral triangle** and all three angles are $60°$. If two sides are of equal length, then it is an **isosceles triangle** and the two angles opposite the equal length sides are equal.

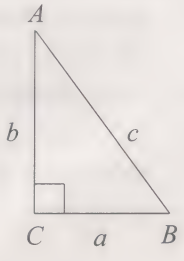
The **area of a triangle** is

- $\frac{1}{2}ah$, where a is the length of the base and h is the height;
- $\frac{1}{2}ab\sin\theta$, where a and b are two side lengths, and θ is the angle between the sides.

Right-angled triangles

Pythagoras' Theorem: For a triangle ABC with side lengths a, b and c (opposite A, B and C, respectively), where the angle at C is a right angle, $c^2 = a^2 + b^2$.

The side opposite the right angle is known as the **hypotenuse**.



For this triangle, the trigonometric ratios are

$$\sin A = \frac{\text{opposite}}{\text{hypotenuse}} = \frac{a}{c}, \quad \cos A = \frac{\text{adjacent}}{\text{hypotenuse}} = \frac{b}{c}, \quad \tan A = \frac{\text{opposite}}{\text{adjacent}} = \frac{a}{b},$$

$$\operatorname{cosec} A = \frac{\text{hypotenuse}}{\text{opposite}} = \frac{c}{a}, \quad \sec A = \frac{\text{hypotenuse}}{\text{adjacent}} = \frac{c}{b}, \quad \cot A = \frac{\text{adjacent}}{\text{opposite}} = \frac{b}{a}.$$

It follows from Pythagoras' Theorem that $\sin^2 A + \cos^2 A = 1$.

Useful trigonometic ratios

Angle θ in radians	0	$\frac{1}{6}\pi$	$\frac{1}{4}\pi$	$\frac{1}{3}\pi$	$\frac{1}{2}\pi$
Angle θ in degrees	0	30	45	60	90
$\sin\theta$	0	$\frac{1}{2}$	$1/\sqrt{2}$	$\sqrt{3}/2$	1
$\cos\theta$	1	$\sqrt{3}/2$	$1/\sqrt{2}$	$\frac{1}{2}$	0
$\tan\theta$	0	$1/\sqrt{3}$	1	$\sqrt{3}$	Undefined

Sine positive	All positive
Tangent positive	Cosine positive

Quadrilaterals

A **quadrilateral** is a polygon with four sides. Its angle sum is 360°, that is, 2π radians.

- ◇ A quadrilateral in which opposite sides are equal is a **parallelogram**.
- ◇ A quadrilateral in which all sides are equal is a **rhombus**.
- ◇ A quadrilateral in which all angles are equal (to 90°) is a **rectangle**.
- ◇ A quadrilateral in which all sides and all angles are equal is a **square**.

In a parallelogram, opposite angles are equal and the two diagonals bisect each other. In a rhombus, the diagonals bisect each other at an angle of 90°.

The area of a rectangle is $A = lb$, where l is the length and b is the breadth.

Circles

A circle of radius r has

- ◇ circumference $C = 2\pi r = \pi d$, where d is the diameter;
- ◇ area $A = \pi r^2$.

Congruence

Two figures are **congruent** if they have the same shape and the same size.

Two n-gons are congruent if all corresponding sides and angles are equal.

Similarity

Two figures are **similar** if they have the same shape; their sizes need not be the same.

Two n-gons are similar if each angle in one n-gon is equal to the corresponding angle in the other. In this case, the length of each side in one n-gon is the same multiple of the corresponding length in the other.

Prisms

A **prism** is a solid with constant cross-section. A **cylinder** is a prism with circular cross-section.

The surface area of a prism is the sum of the areas of its faces. In particular, the surface area of a cylinder is $A = 2\pi r^2 + 2\pi rh$, where r is the radius of the circular cross-section and h is the length.

The volume of a prism is the area of its cross-section multiplied by its length. In particular, the volume of a cylinder is $V = \pi r^2 h$.

Definitions and results in MST121 and MS221

The following definitions and results have been collected from the chapters of MST121 and MS221. They are listed in chapter order with each block of MST121 preceding the corresponding block of MS221 (except that Blocks C of the two courses are combined). If you cannot find the information you want here, then try the alphabetical listing in the Glossary.

MST121 Chapter A1 Sequences

Types of sequences

Convention: The first term of a sequence has subscript 1, unless otherwise indicated.

An **arithmetic sequence** with first term a and common difference d can be specified by either of the following recurrence systems:

◇ $x_1 = a, \quad x_{n+1} = x_n + d \quad (n = 1, 2, 3, \ldots)$,

with closed form $x_n = a + (n-1)d$ $(n = 1, 2, 3, \ldots)$;

◇ $x_0 = a, \quad x_{n+1} = x_n + d \quad (n = 0, 1, 2, \ldots)$,

with closed form $x_n = a + nd$ $(n = 0, 1, 2, \ldots)$.

A **geometric sequence** with first term a and common ratio r can be specified by either of the following recurrence systems:

◇ $x_1 = a, \quad x_{n+1} = rx_n \quad (n = 1, 2, 3, \ldots)$,

with closed form $x_n = ar^{n-1}$ $(n = 1, 2, 3, \ldots)$;

◇ $x_0 = a, \quad x_{n+1} = rx_n \quad (n = 0, 1, 2, \ldots)$,

with closed form $x_n = ar^n$ $(n = 0, 1, 2, \ldots)$.

A **linear recurrence sequence** with parameters a, r and d can be specified by either of the following recurrence systems:

◇ $x_1 = a, \quad x_{n+1} = rx_n + d \quad (n = 1, 2, 3, \ldots)$,

with closed form (when $r \neq 1$)

$$x_n = \left(a + \frac{d}{r-1}\right) r^{n-1} - \frac{d}{r-1} \quad (n = 1, 2, 3, \ldots);$$

◇ $x_0 = a, \quad x_{n+1} = rx_n + d \quad (n = 0, 1, 2, \ldots)$,

with closed form (when $r \neq 1$)

$$x_n = \left(a + \frac{d}{r-1}\right) r^n - \frac{d}{r-1} \quad (n = 0, 1, 2, \ldots).$$

Long-term behaviour of sequences

Range of r	Behaviour of r^n
$r > 1$	$r^n \to \infty$ as $n \to \infty$
$r = 1$	Remains constant: $1, 1, 1, \ldots$
$0 < r < 1$	$r^n \to 0$ as $n \to \infty$
$r = 0$	Remains constant: $0, 0, 0, \ldots$
$-1 < r < 0$	$r^n \to 0$ as $n \to \infty$, alternates in sign
$r = -1$	Alternates between -1 and $+1$
$r < -1$	r^n is unbounded, alternates in sign

Sum of a finite geometric series

The sum of a finite geometric series with first term a and common ratio r ($r \neq 1$) is

$$a + ar + ar^2 + \cdots + ar^n = a\left(\frac{1 - r^{n+1}}{1 - r}\right).$$

MST121 Chapter A2 Lines and circles

Lines

Type	Slope	Equation
Parallel to x-axis	$m = 0$	$y = c$, where c is a constant
Parallel to y-axis	Infinite	$x = d$, where d is a constant
Not parallel to y-axis	$m = (y_2 - y_1)/(x_2 - x_1)$, where (x_1, y_1) and (x_2, y_2) are points on the line	$y - y_1 = m(x - x_1)$ or $y = mx + c$, where c is the y-intercept

If two lines are **parallel**, then they have equal slopes. If two lines are **perpendicular**, then either the product of their slopes is -1 or one has slope 0 and the other has infinite slope.

The **distance** between two points (x_1, y_1) and (x_2, y_2) is

$$\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

The **midpoint** of a line segment with endpoints (x_1, y_1) and (x_2, y_2) is

$$\left(\frac{x_1 + x_2}{2}, \frac{y_1 + y_2}{2}\right).$$

Circles

Geometrically, a **circle** is the set of points that are at a fixed distance (the radius) from a specified point (the centre). Algebraically, a circle with centre (a, b) and radius r has the equation

$$(x - a)^2 + (y - b)^2 = r^2.$$

To find the equation of a circle, given three points A, B and C on the circle, find the perpendicular bisectors of the line segments AB and BC. The centre of the circle is the intersection point of the two perpendicular bisectors. The radius of the circle is the distance from the centre to any of the points A, B or C.

To **complete the square** of $x^2 + 2px$, use

$$x^2 + 2px = x^2 + 2px + p^2 - p^2 = (x + p)^2 - p^2.$$

Trigonometry

Let $P(x, y)$ be a point on the unit circle (with centre O) such that the angle from the positive x-axis to OP is θ (measured anticlockwise if θ is positive, clockwise if θ is negative). Then

$$\cos\theta = x, \qquad \sin\theta = y \quad \text{and} \quad \tan\theta = \frac{\sin\theta}{\cos\theta} \quad \text{(provided that } \cos\theta \neq 0\text{)}.$$

Trigonometric identities

$\cos(-\theta) = \cos\theta$ $\quad$ $\cos(\pi - \theta) = -\cos\theta$ $\quad$ $\cos(\theta + 2\pi) = \cos\theta$

$\sin(-\theta) = -\sin\theta$ $\quad$ $\sin(\pi - \theta) = \sin\theta$ $\quad$ $\sin(\theta + 2\pi) = \sin\theta$

$\tan(-\theta) = -\tan\theta$ $\quad$ $\tan(\pi - \theta) = -\tan\theta$ $\quad$ $\tan(\theta + \pi) = \tan\theta$

$\cos(\frac{1}{2}\pi - \theta) = \sin\theta$ $\quad$ $\sin(\frac{1}{2}\pi - \theta) = \cos\theta$ $\quad$ $\cos^2\theta + \sin^2\theta = 1$

Parametrisation of lines and circles

- A line with slope m passing through the point (x_1, y_1) has parametric equations

  $$x = t + x_1, \quad y = mt + y_1.$$

- A line passing through the two points (x_1, y_1) and (x_2, y_2) has parametric equations

  $$x = x_1 + t(x_2 - x_1), \quad y = y_1 + t(y_2 - y_1).$$

- A circle with centre at (a, b) and radius r has parametric equations

  $$x = a + r\cos\theta, \quad y = b + r\sin\theta \quad (0 \leq \theta \leq 2\pi).$$

MST121 Chapter A3 Functions

Functions

A (**real**) **function** is specified by giving

- the **domain**, that is, the set of allowable input values, which are real numbers;
- the **rule** for converting each input value to a unique output value, which is also a real number.

The output of a function f for a given input x is called the **image** of x under f, and is written $f(x)$. The set of all outputs of the function f is called the **image set** of f.

Convention: When a function is specified just by a rule, it is understood that the domain of the function is the largest possible set of real numbers for which the rule is applicable.

Interval Notation

closed intervals	$a \leq x \leq b$	$[a, b]$
	$a \leq x$	$[a, \infty)$
	$x \leq a$	$(-\infty, a]$
open intervals	$a < x < b$	(a, b)
	$a < x$	(a, ∞)
	$x < a$	$(-\infty, a)$
half open or half closed intervals	$a \leq x < b$	$[a, b)$
	$a < x \leq b$	$(a, b]$

Function notation

A standard notation used to specify a function f is

$$f(x) = x^2 + 1 \quad (0 \leq x \leq 6).$$

Other notations used to specify the same function f are

- $f : x \longmapsto x^2 + 1 \quad (0 \leq x \leq 6)$;
- $f : [0, 6] \longrightarrow \mathbb{R}$
  $x \longmapsto x^2 + 1.$

Modulus of a real number

The **modulus**, or **absolute value**, of a real number x is the magnitude of x, regardless of sign, denoted by $|x|$. Thus

$$|x| = \begin{cases} x, & \text{if } x \geq 0, \\ -x, & \text{if } x < 0. \end{cases}$$

Translating and scaling a known graph

Graph	Translation or scaling of $y = f(x)$
$y = f(x + p)$	Horizontal translation by p units to the left (right if p is negative)
$y = f(x) + q$	Vertical translation by q units upwards (downwards if q is negative)
$y = af(x)$	y-scaling with factor a
$y = f(bx)$	x-scaling with factor $1/b$

Graphing quadratic functions

To sketch the graph of a quadratic function $f(x) = ax^2 + bx + c$, first write the function in completed-square form: $f(x) = a(x + p)^2 + q$. Then start with the graph of $y = x^2$ and perform

1. a y-scaling with factor a;
2. a horizontal translation by p units to the left (right if p is negative);
3. a vertical translation by q units upwards (downwards if q is negative).

The graph is a parabola with vertex $(-p, q)$, which is the lowest point if $a > 0$ and the highest point if $a < 0$. Its axis of symmetry is $x = -p$.

The y-intercept is found by setting $x = 0$ to give $f(0) = c$. The x-intercepts (if any) are found by setting $y = 0$ and solving $ax^2 + bx + c = 0$.

Inverse functions

A real function f is **one-one** if it has the following property: for all x_1, x_2 in the domain of f, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.

A real function f is **increasing** if it has the following property: for all x_1, x_2 in the domain of f, if $x_1 < x_2$, then $f(x_1) < f(x_2)$.

A real function f is **decreasing** if it has the following property: for all x_1, x_2 in the domain of f, if $x_1 < x_2$, then $f(x_1) > f(x_2)$.

If a function is increasing (or decreasing), then it is one-one.

When a function f is one-one, an **inverse function** f^{-1} can be defined which reverses the action of f.

- ◇ To obtain the rule for the function f^{-1}, solve the equation $y = f(x)$ to obtain x in terms of y, and then exchange the roles of x and y. The image set of f is the domain of f^{-1}, and vice versa.
- ◇ To obtain the graph of $y = f^{-1}(x)$, reflect the graph of $y = f(x)$ in the 45° line.

Inverse trigonometric functions

The function $f(x) = \sin x$ $(-\frac{1}{2}\pi \leq x \leq \frac{1}{2}\pi)$ has an inverse function **arcsine** with domain $[-1, 1]$ and image set $[-\frac{1}{2}\pi, \frac{1}{2}\pi]$. Thus, for $-1 \leq y \leq 1$,

$$x = \arcsin y \quad \text{means that} \quad y = \sin x \text{ and } -\tfrac{1}{2}\pi \leq x \leq \tfrac{1}{2}\pi.$$

The function $f(x) = \cos x$ $(0 \leq x \leq \pi)$ has an inverse function **arccosine** with domain $[-1, 1]$ and image set $[0, \pi]$. Thus, for $-1 \leq y \leq 1$,

$$x = \arccos y \quad \text{means that} \quad y = \cos x \text{ and } 0 \leq x \leq \pi.$$

The function $f(x) = \tan x$ $(-\frac{1}{2}\pi < x < \frac{1}{2}\pi)$ has an inverse function **arctangent** with domain $(-\infty, \infty)$ and image set $(-\frac{1}{2}\pi, \frac{1}{2}\pi)$. Thus, for $-\infty < y < \infty$,

$$x = \arctan y \quad \text{means that} \quad y = \tan x \text{ and } -\tfrac{1}{2}\pi < x < \tfrac{1}{2}\pi.$$

Logarithms

An exponential function $f(x) = a^x$, where $a > 0$ and $a \neq 1$, has domain $\mathbb{R}$ and image set $(0, \infty)$. Its inverse function, called **logarithm** to the **base** a and denoted by $\log_a$, has domain $(0, \infty)$ and image set $\mathbb{R}$. Thus, for $y > 0$,

$$x = \log_a y \quad \text{means that} \quad y = a^x.$$

Combining these results gives $x = \log_a(a^x)$, for x in $\mathbb{R}$, and $y = a^{\log_a y}$, for $y > 0$.

The **natural logarithm** has base $e = 2.718\,281\ldots$ and is often written as ln. The **common logarithm** has base 10 and is often written as log.

Provided that $a > 0$ and $a \neq 1$, the logarithm to the base a has the following properties:

(a) $\log_a 1 = 0$, $\log_a a = 1$;

(b) for $x > 0$ and $y > 0$,

(i) $\log_a(xy) = \log_a x + \log_a y$,

(ii) $\log_a(x/y) = \log_a x - \log_a y$;

(c) for $x > 0$ and p in $\mathbb{R}$, $\log_a(x^p) = p \log_a x$.

To use logarithms to solve an equation of the form $a^x = k$, where $k > 0$ and $a > 0, a \neq 1$, apply the function ln to both sides of the equation, and use property (c) to obtain

$$x = \frac{\ln k}{\ln a}.$$

Fibonacci Numbers

n	0	1	2	3	4	5	6	7	8
F_n	0	1	1	2	3	5	8	13	21

MS221 Chapter A1 Exploring sequences

Golden ratio

The **golden ratio equation**, $x^2 - x - 1 = 0$, has solutions $\phi = \frac{1}{2}(1 + \sqrt{5}) \simeq 1.618$ (called the **golden ratio**) and $\psi = \frac{1}{2}(1 - \sqrt{5}) \simeq -0.618$. These solutions have the following properties:

$$\phi + \psi = 1, \qquad \phi\psi = -1, \qquad \phi - \psi = \sqrt{5}, \qquad \phi = 1 + \frac{1}{\phi}, \qquad \psi = 1 + \frac{1}{\psi}.$$

Rationalising the denominator

To **rationalise the denominator** of the fraction $\dfrac{1}{\sqrt{p} + \sqrt{q}}$, multiply both the numerator and the denominator by $\sqrt{p} - \sqrt{q}$.

Properties of solutions of quadratic equations

Let α and β be real solutions of the quadratic equation $ax^2 + bx + c = 0$. Then

$$\alpha + \beta = -\frac{b}{a} \quad \text{and} \quad \alpha\beta = \frac{c}{a}.$$

Fibonacci sequence

The **Fibonacci sequence** is given by

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n \quad (n = 0, 1, 2, \ldots),$$

and has the closed form (**Binet's formula**) $F_n = \dfrac{1}{\sqrt{5}}(\phi^n - \psi^n) \quad (n = 0, 1, 2, \ldots)$.

- ◇ **Binet's approximation** For $n = 0, 1, 2, \ldots$, F_n is the closest integer to $\dfrac{\phi^n}{\sqrt{5}}$.
- ◇ **Fibonacci sum identity** For $n = 0, 1, 2, \ldots$, $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.
- ◇ **Fibonacci ratio property** For $n = 1, 2, 3, \ldots$, the terms of the sequence $\dfrac{F_{n+1}}{F_n}$ lie alternately above and below the golden ratio ϕ and $\dfrac{F_{n+1}}{F_n} \to \phi$ as $n \to \infty$.
- ◇ **Cassini's identity** For $n = 1, 2, 3, \ldots$, $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$.

Linear second-order recurrence sequences

To find a closed form for the linear second-order recurrence sequence given by

$$u_0 = a, \quad u_1 = b, \quad u_{n+2} = pu_{n+1} + qu_n \quad (n = 0, 1, 2, \ldots)$$

when the auxiliary equation has real solutions.

1. Write down the auxiliary equation: $r^2 - pr - q = 0$.
2. Solve the auxiliary equation: $r = \alpha$ and $r = \beta$.
3. Write down the general solution with unknown constants A and B:

$$u_n = \begin{cases} A\alpha^n + B\beta^n, & \text{if } \alpha \text{ and } \beta \text{ are real and distinct,} \\ (A + Bn)\alpha^n, & \text{if } \alpha = \beta. \end{cases}$$

4. Use the initial terms $u_0 = a$ and $u_1 = b$ to find A and B.

MS221 Chapter A2 Conics

Ellipse in standard position

The ellipse with equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \quad (\text{where } a \geq b > 0)$$

- ◇ meets the axes at the points $(a, 0), (-a, 0), (0, b)$ and $(0, -b)$;
- ◇ is symmetric in both the x- and y-axes;
- ◇ can be obtained from the circle $x^2 + y^2 = a^2$ by keeping the x-coordinates of points on the circle unchanged and scaling the y-coordinates by the factor b/a.

Hyperbola in standard position

The hyperbola with equation

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \quad (\text{where } a, b > 0)$$

- ◇ meets the axes at the points $(a, 0)$ and $(-a, 0)$;
- ◇ is symmetric in both the x- and y-axes;
- ◇ is in two unbounded parts, called **branches**, one to the right of $x = a$ and the other to the left of $x = -a$, both with asymptotes $y = \pm(b/a)x$.

Parabola in standard position

The parabola with equation

$$y^2 = 4ax \quad (\text{where } a > 0)$$

- ◇ meets the axes at the point $(0, 0)$;
- ◇ is symmetric in the x-axis and includes the points $(a, 2a)$ and $(a, -2a)$;
- ◇ is in one unbounded part with no asymptotes.

Focus–directrix properties of the non-degenerate conics in standard position

Curve	Equation	Focus	Directrix	Eccentricity
Ellipse	$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ (where $a > b > 0$)	$(\pm ae, 0)$	$x = \pm\frac{a}{e}$	$0 < e < 1$, $e = \sqrt{1 - b^2/a^2}$
Parabola	$y^2 = 4ax$ (where $a > 0$)	$(a, 0)$	$x = -a$	$e = 1$
Hyperbola (asymptotes $y = \pm(b/a)x$)	$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ (where $a, b > 0$)	$(\pm ae, 0)$	$x = \pm\frac{a}{e}$	$e > 1$, $e = \sqrt{1 + b^2/a^2}$

Note that a circle does *not* have a focus–directrix property.

Focus–directrix definitions of the non-degenerate conics in general position

Let F be a point (the focus), d be a line (the directrix) not passing through F, and e be a positive real number (the eccentricity). Then the set of points P satisfying the equation $PF = ePd$ is

$$\begin{cases} \text{an ellipse} & \text{if } 0 < e < 1, \\ \text{a parabola} & \text{if } e = 1, \\ \text{a hyperbola} & \text{if } e > 1. \end{cases}$$

Here Pd is the perpendicular distance from the point P to the line d.

Quadratic curves

A **quadratic curve** is a curve with equation of the form

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0,$$

where A, B, C are not all zero. If $B = 0$, then the curve can usually be obtained by translating a non-degenerate conic in standard position.

Parametrisation of conics in standard position

Curve	Equation	Parametrisation
Ellipse	$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ (where $a \geq b > 0$)	$x = a\cos t, \quad y = b\sin t$ $(0 \leq t \leq 2\pi)$
Parabola	$y^2 = 4ax$ (where $a > 0$)	$x = at^2, \quad y = 2at$
Hyperbola	$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ (where $a, b > 0$)	$x = a\sec t, \quad y = b\tan t$ $(-\frac{1}{2}\pi < t < \frac{1}{2}\pi, \frac{1}{2}\pi < t < \frac{3}{2}\pi)$

MS221 Chapter A3 Functions from geometry

Functions

A general **function** f is defined by specifying a set X, called the **domain** of f, a set Y, called the **codomain** of f, and a rule that associates with each x in X a unique y in Y. This can be expressed as $y = f(x)$, where $f(x)$ is called the **image** of x under f. The set of all such images is called the **image set** of f.

Such general functions are often specified using **two-line notation**:

$$\begin{aligned} f : X &\longrightarrow Y \\ x &\longmapsto f(x). \end{aligned}$$

A **function of two variables** is a function f whose domain is a subset of $\mathbb{R}^2$ and whose codomain is a subset of $\mathbb{R}$. Plotting the points $(x, y, f(x, y))$ in three-dimensional space gives the **graph** of f as a surface lying over the domain, sometimes called a **surface plot**. If the points in the domain at which the function takes a particular value are plotted, then a **contour** is obtained. A collection of contours is called a **contour plot**.

Isometries

An **isometry** (of the plane) is a function with domain and codomain $\mathbb{R}^2$, which preserves the distances between points. Every isometry is one of four basic types: a translation, a rotation, a reflection or a glide-reflection.

Let $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ and $g : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ be two isometries of the plane. Then the **composite** of f followed by g is the isometry $g \circ f$ defined by

$$\begin{aligned} g \circ f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto g(f(x, y)). \end{aligned}$$

A **translation** by p units horizontally and q units vertically is given by

$$\begin{aligned} t_{p,q} : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (x + p, y + q). \end{aligned}$$

The inverse of the translation $t_{p,q}$ is the translation $t_{-p,-q}$. The composite of two translations, $t_{p,q}$ and $t_{r,s}$, is $t_{p,q} \circ t_{r,s} = t_{p+r,q+s}$.

A **rotation** about the origin through an angle θ, measured anticlockwise, is given by

$$\begin{aligned} r_\theta : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta). \end{aligned}$$

The inverse of the rotation r_θ is the rotation $r_{-\theta}$. The composite of two rotations, r_θ and r_ϕ, is $r_\theta \circ r_\phi = r_{\theta+\phi}$.

Let ℓ be a line that passes through the origin and makes an angle θ with the positive x-axis. Then the **reflection** in ℓ is given by

$$\begin{aligned} q_\theta : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (x\cos(2\theta) + y\sin(2\theta), x\sin(2\theta) - y\cos(2\theta)). \end{aligned}$$

All reflections are **self-inverse**.

A **glide-reflection** in a line ℓ is defined to be reflection in ℓ followed by a translation parallel to ℓ.

Trigonometric formulas

Pythagorean identities

$$\cos^2\theta + \sin^2\theta = 1 \qquad 1 + \tan^2\theta = \sec^2\theta \qquad \cot^2\theta + 1 = \operatorname{cosec}^2\theta$$

It follows that

$$\cos\theta = \pm\frac{1}{\sqrt{1+\tan^2\theta}}$$

and

$$\sin\theta = \pm\frac{\tan\theta}{\sqrt{1+\tan^2\theta}}.$$

Sum and difference formulas

$$\sin(\phi+\theta) = \sin\phi\cos\theta + \cos\phi\sin\theta \qquad \sin(\phi-\theta) = \sin\phi\cos\theta - \cos\phi\sin\theta$$

$$\cos(\phi+\theta) = \cos\phi\cos\theta - \sin\phi\sin\theta \qquad \cos(\phi-\theta) = \cos\phi\cos\theta + \sin\phi\sin\theta$$

$$\tan(\phi+\theta) = \frac{\tan\phi + \tan\theta}{1 - \tan\phi\tan\theta} \qquad \tan(\phi-\theta) = \frac{\tan\phi - \tan\theta}{1 + \tan\phi\tan\theta}$$

Double-angle and half-angle formulas

$$\sin(2\theta) = 2\sin\theta\cos\theta$$

$$\begin{aligned} \cos(2\theta) &= \cos^2\theta - \sin^2\theta \\ &= 1 - 2\sin^2\theta \qquad \text{so } \sin^2\theta = \tfrac{1}{2}(1 - \cos(2\theta)) \\ &= 2\cos^2\theta - 1 \qquad \text{so } \cos^2\theta = \tfrac{1}{2}(1 + \cos(2\theta)) \end{aligned}$$

$$\tan(2\theta) = \frac{2\tan\theta}{1 - \tan^2\theta}$$

Sketching a quadratic curve with a cross-term

To sketch a quadratic curve L with equation of the form

$$Ax^2 + Bxy + Cy^2 + F = 0 \quad (\text{where } B \neq 0).$$

1. Find the inclination θ of L, where $-\frac{1}{4}\pi < \theta \leq \frac{1}{4}\pi$, given by

$$\theta = \begin{cases} \frac{1}{4}\pi, & \text{if } A = C, \\ \frac{1}{2}\arctan\left(\dfrac{B}{A-C}\right), & \text{if } A \neq C. \end{cases}$$

2. Obtain the coefficients of the equation $A'x^2 + C'y^2 + F' = 0$ of K, using

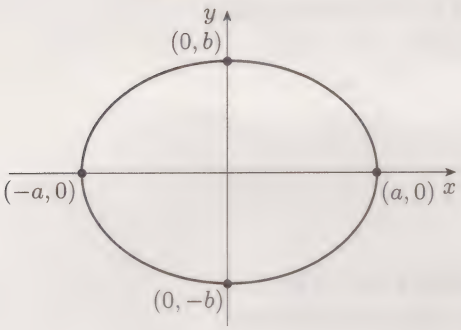
$$A' = A\cos^2\theta + B\sin\theta\cos\theta + C\sin^2\theta,$$
$$C' = A\sin^2\theta - B\sin\theta\cos\theta + C\cos^2\theta,$$
$$F' = F.$$

3. Sketch K, which is usually an ellipse or hyperbola in standard position or in reflected standard position.
4. Sketch $L = r_\theta(K)$ by rotating the sketch of K through the angle θ.

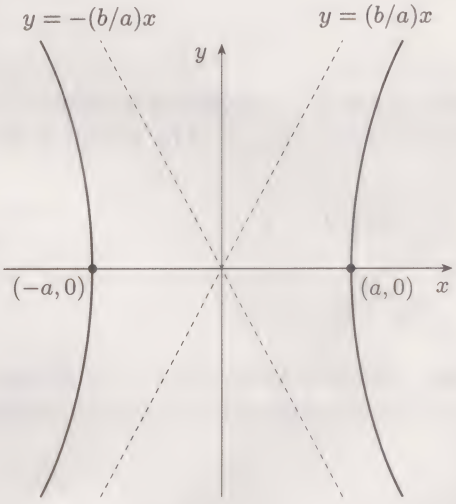
The terms $\cos^2\theta$, $\sin\theta\cos\theta$ and $\sin^2\theta$ can be found directly, without θ, from $\cos(2\theta)$ and $\sin(2\theta)$; these can be obtained from

$$\tan(2\theta) = \frac{B}{A-C}.$$

Ellipse and hyperbola in standard position

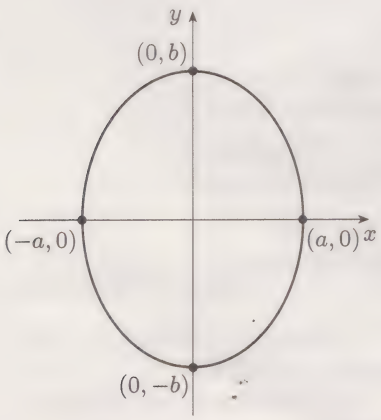


$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \quad (a \geq b > 0)$$

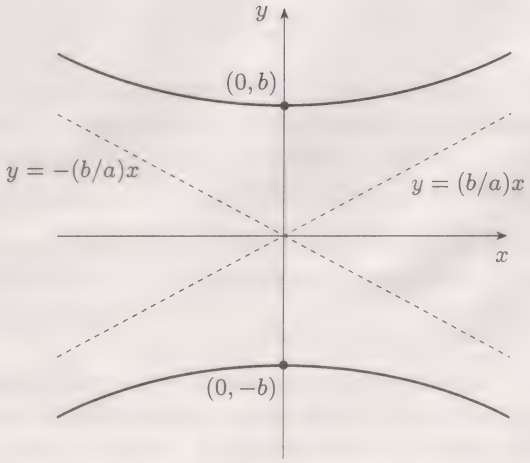


$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \quad (a, b > 0)$$

Ellipse and hyperbola in reflected standard position



$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \quad (b > a > 0)$$



$$-\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \quad (a, b > 0)$$

MST121 Chapter B1 Modelling with sequences

Formulas for sums

$$\sum_{i=1}^{n} c_i = c_1 + c_2 + \cdots + c_n$$

$$\sum_{i=0}^{n} ar^i = a + ar + ar^2 + \cdots + ar^n = a\left(\frac{1 - r^{n+1}}{1 - r}\right) \quad (r \neq 1)$$

$$\sum_{i=0}^{\infty} ar^i = \frac{a}{1 - r} \quad (|r| < 1)$$

$$\sum_{i=1}^{n}(a + bx_i) = an + b\sum_{i=1}^{n} x_i \qquad \sum_{i=m}^{n}(a + bx_i) = a(n - m + 1) + b\sum_{i=m}^{n} x_i$$

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \tfrac{1}{2}n(n + 1)$$

Exponential model

The (discrete) exponential model for population variation is based on the assumption of a constant proportionate growth rate, r. The model is described by either the recurrence relation

$$P_{n+1} = (1 + r)P_n \quad (n = 0, 1, 2, \ldots),$$

or its closed-form solution

$$P_n = (1 + r)^n P_0 \quad (n = 0, 1, 2, \ldots),$$

where P_n is the population size at n years after some chosen starting time. The proportionate growth rate r is the proportionate birth rate minus the proportionate death rate.

Logistic model

The logistic model for population variation is based on the assumption of a proportionate growth rate $R(P)$ of the form $R(P) = r(1 - P/E)$, where r and E are positive parameters. The model is described by the recurrence relation

$$P_{n+1} - P_n = rP_n\left(1 - \frac{P_n}{E}\right) \quad (n = 0, 1, 2, \ldots),$$

where P_n is the population size at n years after some chosen starting time. The positive constant r represents the proportionate growth rate of the population when the population size is small, and the positive constant E represents the equilibrium population level (the population size at which the proportionate growth rate is zero).

The long-term behaviour of sequences generated by the logistic recurrence relation (with $0 < P_0 \leq E(1 + 1/r)$) depends on the value of r, as shown in the table below.

Range of r	Long-term behaviour of P_n
$0 < r \leq 1$	Settles close to (converges to) E, with values always just below E
$1 < r \leq 2$	Settles close to E, with values alternating between just above and just below E
$2 < r \leq 2.44$	2-cycle, with one value above E and one value below E
$2.45 \leq r \leq 2.54$	4-cycle, with two values above E and two values below E
$2.6 \leq r \leq 3$	Chaotic variation between bounds (with some exceptions)

Convergence and limits

If a sequence P_n settles down in the long term to values that are effectively constant, then P_n is said to be **convergent**. The value near which P_n settles in the long term is called the **limit** of the sequence, written

$$\lim_{n\to\infty} P_n.$$

If a sequence P_n given by a recurrence relation converges, then it converges to the value of a constant sequence that satisfies the recurrence relation. To find such values, substitute $P_n = c$ and $P_{n+1} = c$ into the recurrence relation and solve for c.

Reciprocal Rule

If the terms of a sequence b_n are of the form $1/a_n$, where terms of the sequence a_n become arbitrarily large as n increases, then $\lim_{n\to\infty} b_n = 0$.

Constant Multiple Rule

If the terms of a sequence b_n are of the form ca_n, where $\lim_{n\to\infty} a_n = 0$, and c is a constant, then $\lim_{n\to\infty} b_n = 0$.

Long-term 'basic sequence' behaviour

The long-term behaviour of the sequence r^n $(n = 1, 2, 3, \ldots)$ is as follows.

- ◇ If $|r| > 1$, then $|r^n| \to \infty$ as $n \to \infty$. (If $r > 1$, then $r^n \to \infty$ as $n \to \infty$; if $r < -1$, then r^n is unbounded and alternates in sign.)
- ◇ If $|r| < 1$, then $r^n \to 0$ as $n \to \infty$.
- ◇ If $r = 1$, then $r^n = 1$. If $r = -1$, then r^n alternates between 1 and -1.

The long-term behaviour of the sequence n^p $(n = 1, 2, 3, \ldots)$ is as follows.

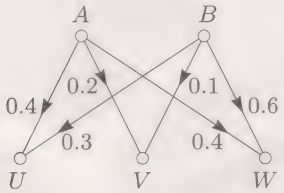
- ◇ If $p > 0$, then $n^p \to \infty$ as $n \to \infty$.
- ◇ If $p < 0$, then $n^p \to 0$ as $n \to \infty$.
- ◇ If $p = 0$, then $n^p = 1$.

MST121 Chapter B2 Modelling with matrices

Networks and matrices

A physical network can be represented by a **network diagram** and also by a matrix. The entries of the matrix indicate the proportion of the input flowing through each pipe of the network.

The network diagram and the matrix shown below represent the same physical network having two input nodes A and B, and three output nodes U, V and W.



$$\begin{pmatrix} 0.4 & 0.3 \\ 0.2 & 0.1 \\ 0.4 & 0.6 \end{pmatrix}$$

If the outputs of one network feed directly into an equal number of inputs in a second network, then the matrix representing the combined network is obtained by multiplying the matrices representing the two original networks.

Arithmetic of matrices and vectors

A **matrix** is a rectangular array of numbers. Each number in a matrix is called an **element**. A matrix with m rows and n columns is called an $m \times n$ matrix, and has **size** $m \times n$. The element in row i and column j of a matrix $\mathbf{A}$ is written as a_{ij}.

Matrix multiplication

Two matrices $\mathbf{A}$ and $\mathbf{B}$ can be multiplied only if the number of columns of $\mathbf{A}$ equals the number of rows of $\mathbf{B}$. The element in the ith row and jth column of the product matrix $\mathbf{AB}$ is obtained by adding up the products of corresponding elements of the ith row of $\mathbf{A}$ and the jth column of $\mathbf{B}$.

Thus, if $\mathbf{A}$ is an $m \times n$ matrix and $\mathbf{B}$ is an $n \times p$ matrix, then $\mathbf{C} = \mathbf{AB}$ is an $m \times p$ matrix with elements given by

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \quad (i = 1, 2, \ldots, m \text{ and } j = 1, 2, \ldots, p).$$

For example, if $\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}$, then

$$\mathbf{C} = \mathbf{AB} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} & a_{11}b_{13} + a_{12}b_{23} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} & a_{21}b_{13} + a_{22}b_{23} \\ a_{31}b_{11} + a_{32}b_{21} & a_{31}b_{12} + a_{32}b_{22} & a_{31}b_{13} + a_{32}b_{23} \end{pmatrix}.$$

In most cases, $\mathbf{AB} \neq \mathbf{BA}$. The **power** $\mathbf{A}^n$ of a square matrix $\mathbf{A}$ is formed by multiplying together n matrices $\mathbf{A}$; for example, $\mathbf{A}^3 = \mathbf{AAA}$.

Matrix addition

Two matrices $\mathbf{A}$ and $\mathbf{B}$ can be added only if they have the same size. If $\mathbf{A}$ and $\mathbf{B}$ are $m \times n$ matrices, then $\mathbf{C} = \mathbf{A} + \mathbf{B}$ is also an $m \times n$ matrix with elements given by

$$c_{ij} = a_{ij} + b_{ij} \quad (i = 1, 2, \ldots, m \text{ and } j = 1, 2, \ldots, n).$$

For example, if $\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}$, then

$$\mathbf{C} = \mathbf{A} + \mathbf{B} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & a_{13} + b_{13} \\ a_{21} + b_{21} & a_{22} + b_{22} & a_{23} + b_{23} \end{pmatrix}.$$

Scalar multiplication

When a matrix is scalar multiplied by a real number k, each element of the matrix is multiplied by k. For example, if

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}, \text{ then } k\mathbf{A} = \begin{pmatrix} ka_{11} & ka_{12} & ka_{13} \\ ka_{21} & ka_{22} & ka_{23} \end{pmatrix}.$$

The matrix $k\mathbf{A}$ is a **scalar multiple** of the matrix $\mathbf{A}$.

General properties of matrices

For any matrices $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ of appropriate size, and any real number k:

$$\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A} \qquad (\mathbf{A} + \mathbf{B}) + \mathbf{C} = \mathbf{A} + (\mathbf{B} + \mathbf{C})$$
$$(\mathbf{AB})\mathbf{C} = \mathbf{A}(\mathbf{BC}) \qquad \mathbf{A}(k\mathbf{B}) = (k\mathbf{A})\mathbf{B} = k(\mathbf{AB})$$
$$\mathbf{AB} + \mathbf{AC} = \mathbf{A}(\mathbf{B} + \mathbf{C})$$

Vectors

A **vector** is a matrix with only one column. Elements of a vector $\mathbf{v}$ are often called **components** and are specified as v_i. The size of a vector is the number of components it has.

For vectors $\mathbf{u}$ and $\mathbf{v}$, the vectors $\mathbf{u}+\mathbf{v}$ and $k\mathbf{u}$ are formed according to the definitions for general matrices.

Population modelling

A matrix model for the structure of a population in terms of two interdependent subpopulations J_n and A_n is given by

$$\mathbf{p}_{n+1} = \mathbf{M}\mathbf{p}_n \quad (n = 0, 1, 2, \ldots),$$

where $\mathbf{M}$ is a 2×2 matrix and $\mathbf{p}_n$ is the vector $\begin{pmatrix} J_n \\ A_n \end{pmatrix}$ which gives the subpopulation sizes at n years after a chosen starting time. The closed-form solution for this model is

$$\mathbf{p}_n = \mathbf{M}^n\mathbf{p}_0 \quad (n = 1, 2, 3, \ldots).$$

Inverting 2 × 2 matrices

The matrix $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the 2×2 **identity matrix**. For any 2×2 matrix $\mathbf{A}$,

$$\mathbf{AI} = \mathbf{IA} = \mathbf{A}.$$

If two 2×2 matrices $\mathbf{A}$ and $\mathbf{B}$ have the property that $\mathbf{AB} = \mathbf{I} = \mathbf{BA}$, then $\mathbf{B}$ is the **inverse** of $\mathbf{A}$. The inverse of a matrix $\mathbf{A}$ is usually denoted $\mathbf{A}^{-1}$. The inverse of the general 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by

$$\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \quad \text{provided } ad - bc \neq 0.$$

The **determinant** of a square matrix is a number calculated from its elements. For a 2×2 matrix $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the determinant is given by $\det \mathbf{A} = ad - bc$.

Determinant test for invertibility

If the determinant of a matrix $\mathbf{A}$ is not zero, then $\mathbf{A}$ has an inverse and $\mathbf{A}$ is **invertible**.
If the determinant of a matrix $\mathbf{A}$ is zero, then $\mathbf{A}$ does not have an inverse and $\mathbf{A}$ is **non-invertible**.

Solving a pair of simultaneous linear equations using matrices

Write the simultaneous linear equations in matrix form $\mathbf{Ax} = \mathbf{b}$, where $\mathbf{A}$ is the coefficient matrix, $\mathbf{x}$ is the vector of variables and $\mathbf{b}$ is the vector with components equal to the right-hand sides of the equations.

If the matrix $\mathbf{A}$ is invertible, then the solution is given by $\mathbf{x} = \mathbf{A}^{-1}\mathbf{b}$.

MST121 Chapter B3 Modelling with vectors

Vectors can be represented: by 2×1 matrices (column form), by arrows in the (x, y)-plane (geometric form), or using the Cartesian unit vectors $\mathbf{i}$ and $\mathbf{j}$ (component form).

Arithmetic of vectors in column form

The **sum** of two vectors with the same number of components is formed by adding the corresponding components.
The **scalar multiple** of a vector $\mathbf{a}$ by a real number (scalar) k, denoted by $k\mathbf{a}$, is formed by multiplying each component of $\mathbf{a}$ by k.

Arithmetic of vectors in geometric form

Triangle Rule

To find the sum $\mathbf{a} + \mathbf{b}$ of two vectors $\mathbf{a}$ and $\mathbf{b}$ in geometric form.

1. Choose any point P in the plane.
2. Draw an arrow to represent $\mathbf{a}$, with tail at P and tip at Q, say.
3. Draw an arrow to represent $\mathbf{b}$, with tail at Q and tip at R, say.
4. Draw the arrow with tail at P and tip at R, to complete the triangle PQR. This last arrow represents the vector $\mathbf{a} + \mathbf{b}$.

Parallelogram Rule

To find the sum $\mathbf{a} + \mathbf{b}$ of two vectors $\mathbf{a}$ and $\mathbf{b}$ in geometric form.

1. Choose any point P in the plane.
2. Draw an arrow to represent $\mathbf{a}$, with tail at P and tip at Q, say.
3. Draw an arrow to represent $\mathbf{b}$, with tail at P and tip at S, say.
4. Complete the parallelogram $PQRS$, and draw the arrow with tail at P and tip at R. This last arrow represents the vector $\mathbf{a} + \mathbf{b}$.

Scalar multiplication

If $\mathbf{a}$ is a vector in geometric form and k is a real number, then the scalar multiple $k\mathbf{a}$ has magnitude $|k\mathbf{a}| = |k||\mathbf{a}|$. If k is non-zero, then the direction of $k\mathbf{a}$ is the same as that of $\mathbf{a}$ if $k > 0$, or opposite to that of $\mathbf{a}$ if $k < 0$.

Arithmetic of vectors in component form

The **sum** of two vectors in component form, $\mathbf{a} = a_1\mathbf{i} + a_2\mathbf{j}$ and $\mathbf{b} = b_1\mathbf{i} + b_2\mathbf{j}$, is given by $\mathbf{a} + \mathbf{b} = (a_1 + b_1)\mathbf{i} + (a_2 + b_2)\mathbf{j}$.

The **scalar multiple** of a vector in component form, $\mathbf{a} = a_1\mathbf{i} + a_2\mathbf{j}$, by a real number k, is given by $k\mathbf{a} = ka_1\mathbf{i} + ka_2\mathbf{j}$.

Converting vectors from geometric form to component form

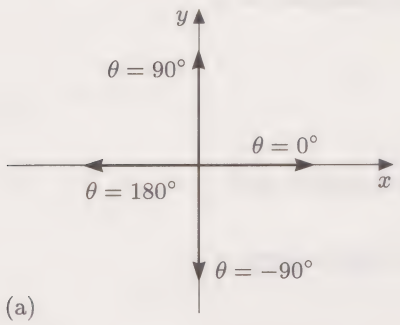
A vector $\mathbf{a}$ in geometric form, with direction θ, has component form

$$\mathbf{a} = |\mathbf{a}| \cos\theta\, \mathbf{i} + |\mathbf{a}| \sin\theta\, \mathbf{j};$$

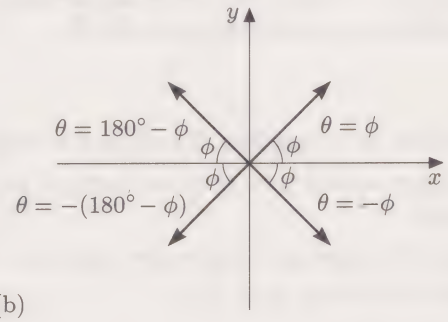
that is, the $\mathbf{i}$-component of $\mathbf{a}$ is $a_1 = |\mathbf{a}| \cos\theta$ and the $\mathbf{j}$-component of $\mathbf{a}$ is $a_2 = |\mathbf{a}| \sin\theta$.

Converting vectors from component form to geometric form

A vector in component form, $\mathbf{a} = a_1\mathbf{i} + a_2\mathbf{j}$, has magnitude $|\mathbf{a}| = \sqrt{a_1^2 + a_2^2}$. If the vector is non-zero, then its direction, in terms of the angle θ measured anticlockwise from the positive x-axis, is obtained from the figures below.



(a)



(b)

(a) $\mathbf{a}$ is parallel to a coordinate axis (b) $\phi = \arctan(|a_2/a_1|)$

Sine and Cosine Rules

By convention, in a triangle, the vertex labels A, B and C are also used to denote the corresponding angle sizes, while the side lengths opposite the angles are denoted by a, b and c, respectively.

In a triangle ABC, if $a < b$ then $A < B$, and vice versa.

Sine Rule

For any triangle, the side lengths a, b, c and corresponding opposite angles A, B, C are related by the formulas

$$\frac{\sin A}{a} = \frac{\sin B}{b} = \frac{\sin C}{c} \quad \text{or, equivalently,} \quad \frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C}.$$

Cosine Rule

For any triangle, the side lengths a, b, c and corresponding opposite angles A, B, C are related by the formulas

$$a^2 = b^2 + c^2 - 2bc\cos A, \qquad \cos A = \frac{b^2 + c^2 - a^2}{2bc},$$

$$b^2 = c^2 + a^2 - 2ca\cos B, \qquad \cos B = \frac{c^2 + a^2 - b^2}{2ca},$$

$$c^2 = a^2 + b^2 - 2ab\cos C, \qquad \cos C = \frac{a^2 + b^2 - c^2}{2ab}.$$

Equilibrium Condition for forces

If an object is acted upon by n forces, $\mathbf{F}_1, \mathbf{F}_2, \ldots, \mathbf{F}_n$, and remains at rest in the absence of other forces, then the force vectors satisfy the equation

$$\sum_{i=1}^{n} \mathbf{F}_i = \mathbf{F}_1 + \mathbf{F}_2 + \cdots + \mathbf{F}_n = \mathbf{0}.$$

MS221 Chapter B1 Iteration

Domain and codomain conventions

When the domain of a real function is not specified, it is understood to be the largest set of real numbers for which the rule is applicable. When the codomain of a real function is not specified, it is understood to be $\mathbb{R}$.

Graphical iteration

To apply graphical iteration to a function f with a starting value x_0.

1. Sketch the graphs of $y = x$ and $y = f(x)$ on a set of axes with equal scales, and mark x_0 on the x-axis.
2. Repeat the following two steps as long as the size and scale of the graph allow.
   (a) Draw a vertical line to meet $y = f(x)$.
   (b) Draw a horizontal line to meet $y = x$.

Two possible patterns found in graphical iteration are staircases and cobwebs. If each vertical line is extended to the x-axis, this graphical construction gives the position on the x-axis of the terms $x_0, x_1, x_2, \ldots$.

Functions

The **gradient** of the graph of the quadratic function $f(x) = ax^2 + bx + c$ at the point $(x, f(x))$ is $f'(x) = 2ax + b$.

A real function f is **increasing on an interval** I if it has the property that for all x_1, x_2 in I, if $x_1 < x_2$, then $f(x_1) < f(x_2)$.

A real function f is **decreasing on an interval** I if it has the property that for all x_1, x_2 in I, if $x_1 < x_2$, then $f(x_1) > f(x_2)$.

Let two functions $f : A \longrightarrow B$ and $g : C \longrightarrow D$ have the property that the image set $f(A)$ is a subset of C. Then the **composite function** $g \circ f$ is defined by

$$\begin{aligned} g \circ f : A &\longrightarrow D \\ x &\longmapsto g(f(x)). \end{aligned}$$

Fixed points

A **fixed point** of a real function f is a number a in the domain of f such that $f(a) = a$. To find the fixed points of f, solve the fixed point equation $f(x) = x$.

Fixed point rule

Suppose that x_n is a sequence obtained by iteration of a continuous real function f, and that x_n converges to the limit ℓ, which is in the domain of f. Then ℓ is a fixed point of f.

Behaviour near an attracting or repelling fixed point

Let a be a fixed point of a smooth function f, and let x_n be an iteration sequence generated by f.

- ◇ If $|f'(a)| < 1$, then there is an open interval I containing a with the property that if x_0 is in I, then $x_n \to a$ as $n \to \infty$.
- ◇ If $|f'(a)| > 1$, then x_n does not tend to a unless $x_n = a$ for some value of n.

Classification of fixed points

A fixed point a of a smooth function f can be classified as follows:

- ◇ a is an **attracting** fixed point if $|f'(a)| < 1$;
- ◇ a is a **repelling** fixed point if $|f'(a)| > 1$;
- ◇ a is an **indifferent** fixed point if $|f'(a)| = 1$;
- ◇ a is a **super-attracting** fixed point if $f'(a) = 0$.

Interval of attraction: graphical criterion

Suppose that f is a smooth function with an attracting fixed point a. If I is an open interval on which f is increasing and a is the only fixed point of f in I, then I is an interval of attraction for a.

Interval of attraction: gradient criterion

Suppose that f is a smooth function with an attracting fixed point a. If I is an open interval with midpoint a such that

$$|f'(x)| < 1 \quad \text{for } x \in I,$$

then I is an interval of attraction for a.

To find an interval of attraction using the gradient criterion, determine the set of points x which satisfy the inequalities $-1 < f'(x) < 1$, and then choose an open interval from this set with midpoint a.

2-cycles

A **2-cycle** of a real function f is a pair of distinct numbers a and b in the domain of f such that $f(a) = b$ and $f(b) = a$. To find any 2-cycles of a real function f, solve the 2-cycle equation $f(f(x)) = x$. The solutions of this 2-cycle equation are either fixed points of f or members of 2-cycles of f.

2-cycle rule

Suppose that the sequence x_n is generated by iteration of the real function f and that

the sequence $x_0, x_2, x_4, \ldots$ tends to a,
the sequence $x_1, x_3, x_5, \ldots$ tends to b,

where $a \neq b$. If f is continuous, then a and b form a 2-cycle of the function f.

Behaviour near an attracting or repelling 2-cycle

Let a, b be a 2-cycle of the smooth function f, and let x_n be an iteration sequence generated by f.

- ◇ If $|f'(a)f'(b)| < 1$, then there is an open interval I containing a with the property that if x_0 is in I, then

  the sequence $x_0, x_2, x_4, \ldots$ tends to a,
  the sequence $x_1, x_3, x_5, \ldots$ tends to b.

- ◇ If $|f'(a)f'(b)| > 1$, then x_n does not tend to the 2-cycle a, b unless $x_n = a$ for some value of n.

Classification of 2-cycles

A 2-cycle a, b of a smooth function f can be classified as follows:

- a, b is an **attracting** 2-cycle if $|f'(a)f'(b)| < 1$;
- a, b is a **repelling** 2-cycle if $|f'(a)f'(b)| > 1$;
- a, b is an **indifferent** 2-cycle if $|f'(a)f'(b)| = 1$;
- a, b is a **super-attracting** 2-cycle if $f'(a)f'(b) = 0$.

Number of members of p-cycle is no. of vertical construction lines on graph

p-cycles

Distinct numbers $a_1, a_2, \ldots, a_p$ in the domain of a real function f form a ***p*-cycle** of f if

$$f(a_1) = a_2, \quad f(a_2) = a_3, \quad \ldots, \quad f(a_p) = a_1.$$

Let μ be the gradient product $f'(a_1)f'(a_2)\cdots f'(a_p)$. Then the p-cycle is **attracting** if $|\mu| < 1$, **repelling** if $|\mu| > 1$, **indifferent** if $|\mu| = 1$, and **super-attracting** if $\mu = 0$.

The numbers $a_1, a_2, \ldots, a_p$ in the p-cycle are fixed points of the composite function $f \circ f \circ \cdots \circ f$, often denoted f^p. This function is called the ***p*th iterate** of f.

Permutations and combinations

A **permutation** of n objects taken k at a time is an arrangement formed by choosing k objects from n objects (all different) and placing them in a particular order. The number of permutations of n objects taken k at a time is

$${}^nP_k = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}.$$

A **combination** of n objects taken k at a time is a selection of k objects from n objects (all different) in which order does not matter. The number of combinations of n objects taken k at a time is

$${}^nC_k = \frac{{}^nP_k}{k!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{(n-k)!k!}.$$

For example,

$${}^nC_0 = 1, \quad {}^nC_1 = n, \quad {}^nC_2 = \frac{n(n-1)}{2!}, \quad {}^nC_3 = \frac{n(n-1)(n-2)}{3!}.$$

Properties of ${}^nC_k$

$${}^nC_k = {}^nC_{n-k}, \qquad {}^nC_{k+1} = {}^nC_k\left(\frac{n-k}{k+1}\right).$$

The Binomial Theorem

For $n = 1, 2, 3, \ldots,$

$$(a+b)^n = a^n + {}^nC_1a^{n-1}b + \cdots + {}^nC_ka^{n-k}b^k + \cdots + b^n.$$

The numbers ${}^nC_k$ are called **binomial coefficients**.

MS221 Chapter B2 Matrix Transformations

Vectors in the plane

Let $P(x, y)$ be any point in the plane, and O be the origin. Then the vector $\overrightarrow{OP}$ is called the **position vector of** P **(with respect to** O**)**. The position vector $\overrightarrow{OP}$ is usually denoted by the corresponding lower-case letter $\mathbf{p}$, so $\overrightarrow{OP} = \mathbf{p} = \begin{pmatrix} x \\ y \end{pmatrix}$.

A **translation** of the plane through the vector $\mathbf{a} = \begin{pmatrix} p \\ q \end{pmatrix}$ has the form

$$\begin{aligned} t_{p,q} : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ \mathbf{x} &\longmapsto \mathbf{x} + \mathbf{a}. \end{aligned}$$

Linear transformations

A **linear transformation** of the plane is a function of the form

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ \mathbf{x} &\longmapsto \mathbf{A}\mathbf{x}, \end{aligned}$$

where $\mathbf{A}$ is a 2×2 matrix. The linear transformation f is said to be *represented* by the matrix $\mathbf{A}$.

Basic linear transformations

A **rotation** about the origin through an angle θ radians has the form

$$\begin{aligned} r_\theta : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ \mathbf{x} &\longmapsto \mathbf{R}_\theta \mathbf{x}, \end{aligned} \qquad \text{where } \mathbf{R}_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

A **reflection** in the line through the origin which makes an angle θ radians with the positive x-axis has the form

$$\begin{aligned} q_\theta : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ \mathbf{x} &\longmapsto \mathbf{Q}_\theta \mathbf{x}, \end{aligned} \qquad \text{where } \mathbf{Q}_\theta = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}.$$

A **scaling** with **factors** a and b, where $a \neq 0$, $b \neq 0$, is a linear transformation

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ \mathbf{x} &\longmapsto \mathbf{A}\mathbf{x}, \end{aligned} \qquad \text{where } \mathbf{A} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

A **uniform scaling** with **factor** a is a scaling with both factors equal to a.

An ***x*-shear** with **factor** a, where $a \in \mathbb{R}$, is a linear transformation

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ \mathbf{x} &\longmapsto \mathbf{A}\mathbf{x}, \end{aligned} \qquad \text{where } \mathbf{A} \text{ is the matrix } \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

A ***y*-shear** with **factor** a, where $a \in \mathbb{R}$, is a linear transformation

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ \mathbf{x} &\longmapsto \mathbf{A}\mathbf{x}, \end{aligned} \qquad \text{where } \mathbf{A} \text{ is the matrix } \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

A **flattening** is a linear transformation

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ \mathbf{x} &\longmapsto \mathbf{A}\mathbf{x}, \end{aligned}$$

for which $\det \mathbf{A} = 0$ or, equivalently, one column of $\mathbf{A}$ is a scalar multiple (possibly a zero multiple) of the other.

Properties of linear transformations

Linear transformations preserve linearity

Let f be a linear transformation represented by a 2×2 matrix $\mathbf{A}$, other than the zero matrix. Let ℓ be a line through a point P in the direction of a vector $\mathbf{u}$. Then the image $f(\ell)$ is a line through the point $f(P)$ in the direction of the vector $\mathbf{Au}$.

Linear transformations preserve parallelism

Let f be a linear transformation represented by a 2×2 matrix $\mathbf{A}$, other than the zero matrix. Let ℓ_1 and ℓ_2 be two parallel lines. Then the image lines $f(\ell_1)$ and $f(\ell_2)$ are also parallel.

Images of (0, 0), (1, 0) and (0, 1)

If f is the linear transformation represented by the matrix $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then f maps $(0,0)$ to $(0,0)$, $(1,0)$ to (a,c) and $(0,1)$ to (b,d).

Areas and orientation

Under a linear transformation f, the areas of figures are scaled by a factor equal to the area of the image of the unit square. If f is the linear transformation represented by the matrix $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then f scales areas by the factor $|\det \mathbf{A}| = |ad - bc|$. The orientation of a figure is preserved if $\det \mathbf{A}$ is positive, and reversed if $\det \mathbf{A}$ is negative.

One-one and onto functions

A function $f : A \longrightarrow B$ is **one-one** (or **one-to-one**) if each element of $f(A)$ is the image of exactly one element of A; that is,

for all $a, b \in A$, if $a \neq b$, then $f(a) \neq f(b)$.

A function that is not one-one is **many-one**.

To prove that a linear transformation $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is one-one, suppose that (r, s) and (u, v) are two points such that $f(r, s) = f(u, v)$, and deduce that $(r, s) = (u, v)$.

A function $f : A \longrightarrow B$ is **onto** if $f(A) = B$.

To prove that a linear transformation $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is onto, show that for each point (u, v) in the codomain $\mathbb{R}^2$, there is a point (x, y) in the domain $\mathbb{R}^2$ such that $f(x, y) = (u, v)$.

Composites and inverses of linear transformations

If $f(\mathbf{x}) = \mathbf{Ax}$ and $g(\mathbf{x}) = \mathbf{Bx}$ are two linear transformations, then the **composite** function $g \circ f$ is the linear transformation represented by the matrix $\mathbf{BA}$.

Let f be a linear transformation of the plane, represented by a matrix $\mathbf{A}$. If $\mathbf{A}$ is invertible, then f is a one-one, onto function with **inverse** f^{-1}. This inverse is a linear transformation represented by the matrix $\mathbf{A}^{-1}$. Then f is said to be **invertible** (or non-singular). If the matrix $\mathbf{A}$ is not invertible, then f is a many-one function that flattens the plane, so f has no inverse.

Composition of rotations and reflections

$r_\theta \circ r_\phi = r_{\theta+\phi}, \quad q_\theta \circ q_\phi = r_{2(\theta-\phi)}.$

Determinants

Let $\mathbf{A}$ and $\mathbf{B}$ be 2×2 matrices. Then $\det(\mathbf{BA}) = \det \mathbf{B} \det \mathbf{A}$.

If $\mathbf{A}$ is an invertible matrix, then $\det(\mathbf{A}^{-1}) = \dfrac{1}{\det \mathbf{A}}$.

Affine transformations

An **affine transformation** of the plane is a function of the form

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$
$$\mathbf{x} \longmapsto \mathbf{Ax} + \mathbf{a},$$

where $\mathbf{A}$ is a 2×2 matrix and $\mathbf{a}$ is a vector with two components.

The affine transformation $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ that maps the points $(0,0)$, $(1,0)$, $(0,1)$ to the points (p,q), (s,t), (u,v), respectively, is given by

$$f(\mathbf{x}) = \begin{pmatrix} s-p & u-p \\ t-q & v-q \end{pmatrix} \mathbf{x} + \begin{pmatrix} p \\ q \end{pmatrix}.$$

MS221 Chapter B3 Iteration with matrices

Fixed points and invariant lines

A **fixed point** of a linear transformation represented by the matrix $\mathbf{A}$ is a point, represented by the vector $\mathbf{x}$, such that $\mathbf{Ax} = \mathbf{x}$.

An **invariant line** of a linear transformation is a line that is equal to its image under the linear transformation.

Fixed points and invariant lines through the origin O of basic linear transformations are as follows.

Basic linear transformation	Conditions	Fixed points	Invariant lines through O
Rotation about O through angle θ	$\theta = k\pi$, $k \in \mathbb{Z}$, k even $\theta = k\pi$, $k \in \mathbb{Z}$, k odd Other θ	All O O	All All None
Reflection in a line through O	Every reflection	Axis of reflection	Axis of reflection and line perpendicular to it
Scaling with factors a and b	$a, b \neq 1$, $a \neq b$ $a, b \neq 1$, $a = b$ $a = 1$, $b \neq 1$ $a \neq 1$, $b = 1$ $a = b = 1$	O O x-axis y-axis All	x- and y-axes All x- and y-axes x- and y-axes All
x- or y-shear with factor a	$a = 0$ x-shear, $a \neq 0$ y-shear, $a \neq 0$	All x-axis y-axis	All x-axis y-axis

Eigenvalues, eigenlines and eigenvectors

Let $\mathbf{A}$ be a 2×2 matrix. If $\mathbf{x}$ is a non-zero vector representing a point (x, y) and k is a real number such that $\mathbf{Ax} = k\mathbf{x}$, then k is called an **eigenvalue** of $\mathbf{A}$ (or of the linear transformation represented by $\mathbf{A}$) and $\mathbf{x}$ is called an **eigenvector** of $\mathbf{A}$ (or of the linear transformation represented by $\mathbf{A}$). The line through the origin on which an eigenvector lies is called an **eigenline**.

Diagonal and triangular matrices have their eigenvalues on the leading diagonal.

To find the eigenvalues, eigenlines and eigenvectors of the matrix $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

1. Solve the **characteristic equation** $k^2 - (a + d)k + ad - bc = 0$ to find any eigenvalues k. If there are no real solutions to this equation, then there are no eigenvalues.
2. For each eigenvalue k found in Step 1:
   (a) substitute the eigenvalue k into the **eigenvector equation** $\mathbf{Ax} = k\mathbf{x}$, where $\mathbf{x}$ is the vector $\begin{pmatrix} x \\ y \end{pmatrix}$;
   (b) use the simultaneous equations given by the eigenvector equation to find the equation of the eigenline;
   (c) choose a convenient non-zero vector on the eigenline as an eigenvector.

Diagonalising a matrix

To express a 2×2 matrix $\mathbf{A}$, which has distinct eigenvalues, in the form $\mathbf{PDP}^{-1}$, where $\mathbf{D}$ is a diagonal matrix.

1. Find the eigenvalues k_1 and k_2 of $\mathbf{A}$.
2. Define the diagonal matrix $\mathbf{D} = \begin{pmatrix} k_1 & 0 \\ 0 & k_2 \end{pmatrix}$.
3. Find the eigenlines corresponding to the eigenvalues k_1 and k_2.
4. Choose
   - ◇ an eigenvector $\begin{pmatrix} p_1 \\ q_1 \end{pmatrix}$ for the eigenvalue k_1,
   - ◇ an eigenvector $\begin{pmatrix} p_2 \\ q_2 \end{pmatrix}$ for the eigenvalue k_2.
5. Use these eigenvectors to define the matrix $\mathbf{P} = \begin{pmatrix} p_1 & p_2 \\ q_1 & q_2 \end{pmatrix}$.
6. Calculate the matrix $\mathbf{P}^{-1}$.

Then $\mathbf{A} = \mathbf{PDP}^{-1}$.

Matrix powers

If a 2×2 matrix $\mathbf{A}$ can be written in the form $\mathbf{A} = \mathbf{PDP}^{-1}$, where $\mathbf{D}$ is a diagonal matrix, then

$$\mathbf{A}^n = \mathbf{PD}^n\mathbf{P}^{-1}, \quad \text{for } n = 1, 2, 3, \ldots.$$

Properties of generalised scalings

Let the linear transformation f be represented by a 2×2 matrix $\mathbf{A}$ that has two distinct non-zero eigenvalues k_1 and k_2 with corresponding eigenlines ℓ_1 and ℓ_2 (that is, f is a generalised scaling). Let P be a point of $\mathbb{R}^2$ with image P' under f.

(a) (i) If $k_1 > 0$, then P' lies on the same side of ℓ_2 as P.
(ii) If $k_1 < 0$, then P' lies on the opposite side of ℓ_2 to P.

(b) The distance from P' to ℓ_2 is $|k_1|$ times the distance from P to ℓ_2.

Iteration properties of generalised scalings

Initial point on an eigenline

Let $\mathbf{x}_n$ be an iteration sequence generated by the matrix $\mathbf{A}$ of a generalized scaling, with the initial non-zero point $\mathbf{x}_0$ on an eigenline ℓ that corresponds to a (non-zero) eigenvalue k of $\mathbf{A}$. The table below gives the long-term behaviour of $\mathbf{x}_n$.

k	Long-term behaviour of $\mathbf{x}_n$ on ℓ
$k > 1$	$\mathbf{x}_n$ moves away from $(0,0)$, on the same half of ℓ as $\mathbf{x}_0$
$k = 1$	$\mathbf{x}_n = \mathbf{x}_0$, for $n = 0, 1, 2, \ldots$ (a constant sequence)
$0 < k < 1$	$\mathbf{x}_n$ moves towards $(0,0)$, on the same half of ℓ as $\mathbf{x}_0$
$-1 < k < 0$	$\mathbf{x}_n$ moves towards $(0,0)$, alternating between the halves of ℓ
$k = -1$	$\mathbf{x}_n$ alternates between $\pm\mathbf{x}_0$
$k < -1$	$\mathbf{x}_n$ moves away from $(0,0)$, alternating between the halves of ℓ

Initial point not on an eigenline

Let the linear transformation f be represented by a 2×2 matrix $\mathbf{A}$ that has two distinct non-zero eigenvalues k_1 and k_2 with corresponding eigenlines ℓ_1 and ℓ_2. Let (x_0, y_0) be a point of $\mathbb{R}^2$ which is not on an eigenline of $\mathbf{A}$, and let (x_n, y_n) be an iteration sequence generated by $\mathbf{A}$, with initial point (x_0, y_0).

(a) (i) If $k_1 > 0$, then all the points of (x_n, y_n) lie on the same side of ℓ_2 as (x_0, y_0).
(ii) If $k_1 < 0$, then the points of (x_n, y_n) alternate between opposite sides of ℓ_2.

(b) (i) If $\max\{|k_1|, |k_2|\} > 1$, then the sequence moves away from $(0,0)$.
(ii) If $\max\{|k_1|, |k_2|\} < 1$, then the sequence moves towards $(0,0)$.

(c) If $|k_1| > |k_2|$, then

$$\frac{y_n}{x_n} \to m \text{ as } n \to \infty,$$

where m is the gradient of ℓ_1. (If ℓ_1 is the y-axis, then $y_n/x_n \to \infty$ as $n \to \infty$.)

Property (c) is called the **Dominant Eigenvalue Property**; k_1 is called the **dominant eigenvalue** and ℓ_1 is called the **dominant eigenline**.

MST121–MS221 Combined Chapters C1 Differentiation

Differentiation (MST121–MS221)

Differentiation is a process which enables you to find: the gradient of a graph, and the rate at which one variable changes with respect to another.

Let f be a function.

◇ The **derivative** $f'(x)$ at a point x in the domain of f is the gradient of the graph of f at $(x, f(x))$, given by

$$f'(x) = \lim_{h \to 0} \left(\frac{f(x+h) - f(x)}{h} \right),$$

provided that this limit exists.

◇ If $y = f(x)$, then $f'(x)$ is the **rate of change** of y with respect to x.

A function is said to be *smooth* if its derivative exists at each point of its domain.

In Leibniz notation, $f'(x)$ is $\dfrac{d}{dx}(f(x))$, or $\dfrac{dy}{dx}$ where $y = f(x)$.

In Newton's notation, $\dfrac{ds}{dt} = \dot{s}$ (used only when differentiating with respect to time).

Table of standard derivatives (MST121–MS221)

Function $f(x)$		Derivative $f'(x)$	
c		0	
x^n		nx^{n-1}	
$\sin(ax)$		$a\cos(ax)$	
$\cos(ax)$		$-a\sin(ax)$	
e^{ax}		ae^{ax}	
$\ln(ax)$	$(ax > 0)$	$1/x$	$(ax > 0)$
$\tan x$		$\sec^2 x$	
$\cot x$		$-\operatorname{cosec}^2 x$	
$\sec x$		$\sec x \tan x$	
$\operatorname{cosec} x$		$-\operatorname{cosec} x \cot x$	
$\arcsin x$		$\dfrac{1}{\sqrt{1-x^2}}$	$(-1 < x < 1)$
$\arccos x$		$-\dfrac{1}{\sqrt{1-x^2}}$	$(-1 < x < 1)$
$\arctan x$		$\dfrac{1}{1+x^2}$	

Sum and Constant Multiple Rules (MST121–MS221)

If k is a function with rule of the form $k(x) = f(x) + g(x)$, where f and g are smooth functions, then k is smooth and

$$k'(x) = f'(x) + g'(x).$$

If k is a function with rule of the form $k(x) = cf(x)$, where f is a smooth function and c is a constant, then k is smooth and

$$k'(x) = cf'(x).$$

Product Rule (MST121–MS221)

If k is a function with rule of the form $k(x) = f(x)g(x)$, where f and g are smooth functions, then k is smooth and

$$k'(x) = f'(x)g(x) + f(x)g'(x).$$

In Leibniz notation, if $y = uv$, where $u = f(x)$ and $v = g(x)$, then

$$\frac{dy}{dx} = \frac{du}{dx}v + u\frac{dv}{dx}.$$

Quotient Rule (MST121–MS221)

If k is a function with rule of the form $k(x) = f(x)/g(x)$, where f and g are smooth functions, then k is smooth and

$$k'(x) = \frac{g(x)f'(x) - f(x)g'(x)}{(g(x))^2}.$$

In Leibniz notation, if $y = u/v$, where $u = f(x)$ and $v = g(x) \neq 0$, then

$$\frac{dy}{dx} = \frac{1}{v^2}\left(v\frac{du}{dx} - u\frac{dv}{dx}\right).$$

Composite Rule (MST121–MS221)

If k is a function with rule of the form $k(x) = g(f(x))$, where f and g are smooth functions, then k is smooth and

$$k'(x) = g'(f(x))f'(x).$$

In Leibniz notation (Chain Rule), if $y = g(u)$, where $u = f(x)$, then

$$\frac{dy}{dx} = \frac{dy}{du}\frac{du}{dx}.$$

Inverse Rule (MS221)

If g is a function with rule of the form $g(x) = f^{-1}(x)$, where f is a smooth function, then

$$g'(x) = (f^{-1})'(x) = \frac{1}{f'(g(x))}, \quad \text{provided that } f'(g(x)) \neq 0.$$

In Leibniz notation, if $y = g(x)$ where $g = f^{-1}$, so $x = f(y)$, then

$$\frac{dy}{dx} = 1/\frac{dx}{dy}, \text{ provided that } \frac{dx}{dy} \neq 0.$$

Some important limits (MS221)

$$\lim_{h\to 0}\left(\frac{\cos h - 1}{h}\right) = 0 \qquad \lim_{h\to 0}\left(\frac{\sin h}{h}\right) = 1 \qquad \lim_{h\to 0}\left(\frac{e^h - 1}{h}\right) = 1$$

Increasing/Decreasing Criterion (MST121–MS221)

Let I be an open interval in the domain of a smooth function f.

- ◇ If $f'(x) > 0$ for all x in I, then f is increasing on I.
- ◇ If $f'(x) < 0$ for all x in I, then f is decreasing on I.

Stationary points (MST121–MS221)

Let f be a smooth function. The function f has a **stationary point** at $x = x_0$ if $f'(x_0) = 0$. The corresponding point $(x_0, f(x_0))$ on the graph of f is also called a stationary point.

First Derivative Test (MST121–MS221)

Suppose that x_0 is a stationary point of a smooth function f; that is, $f'(x_0) = 0$.

- ◇ If $f'(x)$ changes sign from positive to negative as x increases through x_0, then f has a local maximum at x_0.
- ◇ If $f'(x)$ changes sign from negative to positive as x increases through x_0, then f has a local minimum at x_0.
- ◇ If $f'(x)$ does not change sign as x increases through x_0, then f has neither a local maximum nor a local minimum at x_0.

To determine whether the derivative changes sign as x increases through x_0, either use a sign table for $f'(x)$ or use test points as follows:

(a) choose points x_L to the left of x_0 and x_R to the right of x_0, such that the interval $[x_L, x_R]$ lies in the domain of f and there are no stationary points between x_L and x_0, nor between x_0 and x_R, and then calculate $f'(x_L)$ and $f'(x_R)$;

(b) classify x_0 as follows:

- ◇ if $f'(x_L) > 0$ and $f'(x_R) < 0$, then f has a local maximum at x_0;
- ◇ if $f'(x_L) < 0$ and $f'(x_R) > 0$, then f has a local minimum at x_0;
- ◇ if $f'(x_L)$ and $f'(x_R)$ have the same sign, then f has neither a local maximum nor a local minimum at x_0.

Second Derivative Test (MST121–MS221)

Suppose that x_0 is a stationary point of a smooth function f; that is, $f'(x_0) = 0$.

- ◇ If $f''(x_0) < 0$, then f has a local maximum at x_0.
- ◇ If $f''(x_0) > 0$, then f has a local minimum at x_0.

Optimisation Procedure (MST121)

To find the greatest (or least) value of a smooth function f on a closed interval I within the domain of f, proceed as follows.

1. Find the stationary points of f.
2. Evaluate f at each of the endpoints of I and at each of the stationary points inside I.
3. Choose the greatest (or least) of the function values found in Step 2.

Asymptotic behaviour of polynomial functions (MS221)

The asymptotic behaviour of a polynomial function of degree n,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $n \geq 1$ and $a_n \neq 0$, is similar to that of the function $g(x) = a_n x^n$. The asymptotic behaviour of $f(x)$, for $a_n > 0$, is described in the following table.

$a_n > 0$	$x \to \infty$	$x \to -\infty$
n even	$f(x) \to \infty$	$f(x) \to \infty$
n odd	$f(x) \to \infty$	$f(x) \to -\infty$

Asymptotic behaviour of rational functions (MS221)

A **vertical** asymptote of a rational function $f(x) = p(x)/q(x)$ occurs at those points a for which $q(a) = 0$ and $p(a) \neq 0$. To detect **horizontal** asymptotes of $f(x)$, divide both the numerator and the denominator by the dominant term of the denominator, and consider the behaviour as $x \to \infty$ and as $x \to -\infty$.

Graph-sketching strategy (MS221)

To sketch the graph of a given function f, determine the following features of f (where possible) and then show these features in your sketch.

1. The domain of f.
2. Whether f is even or odd.
3. The x- and y-intercepts of f.
4. The intervals on which f is positive or negative.
5. The intervals on which f is increasing or decreasing and any stationary points, local maxima and local minima.
6. The asymptotic behaviour of f.

Newton–Raphson method (MS221)

Let f be a smooth function. The Newton–Raphson method for finding an approximate solution of the equation $f(x) = 0$ is to start with an initial term x_0 (preferably near a zero of f) and calculate the iteration sequence given by

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \quad (n = 0, 1, 2, \ldots).$$

The Newton–Raphson method may fail to converge to a zero of f; for example, a term x_n may be a stationary point of f, the sequence x_n may converge to a p-cycle, $p \geq 2$, or the sequence x_n may tend to infinity.

MST121–MS221 Combined Chapters C2 Integration

Integration (MST121–MS221)

The function F is an **integral** (or **antiderivative**) of the function f over the interval I if $F'(x) = f(x)$ for all $x \in I$. The **indefinite integral** of $f(x)$ over I is

$$\int f(x)\,dx = F(x) + c \quad (x \in I),$$

where F is an integral of f and c is an arbitrary constant, also called the **constant of integration**.

The **definite integral** of a continuous function f from a to b, denoted by

$$\int_a^b f(x)\,dx \quad \text{or by} \quad \int_a^b f,$$

is defined to be

$$[F(x)]_a^b = F(b) - F(a),$$

where F is any integral of f over an interval I and $a, b \in I$.

Table of indefinite integrals (MST121–MS221)

Function $f(x)$		Integral $\int f(x)\,dx$
a	(constant)	$ax + c$
x^n	$(n \neq -1)$	$\frac{1}{n+1}x^{n+1} + c$
$\frac{1}{x}$		$\ln\lvert x\rvert + c$
e^{ax}		$\frac{1}{a}e^{ax} + c$
$\cos(ax)$		$\frac{1}{a}\sin(ax) + c$
$\sin(ax)$		$-\frac{1}{a}\cos(ax) + c$
$\sec^2(ax)$		$\frac{1}{a}\tan(ax) + c$
$\operatorname{cosec}^2(ax)$		$-\frac{1}{a}\cot(ax) + c$
$\sec(ax)\tan(ax)$		$\frac{1}{a}\sec(ax) + c$
$\operatorname{cosec}(ax)\cot(ax)$		$-\frac{1}{a}\operatorname{cosec}(ax) + c$
$\frac{1}{\sqrt{1-x^2}}$		$\arcsin x + c$
$-\frac{1}{\sqrt{1-x^2}}$		$\arccos x + c$
$\frac{1}{1+x^2}$		$\arctan x + c$

Rules for integration (MST121–MS221)

The **Sum Rule** for integrals is

$$\int (f(x) + g(x))\,dx = \int f(x)\,dx + \int g(x)\,dx.$$

The **Constant Multiple Rule** for integrals is

$$\int kf(x)\,dx = k\int f(x)\,dx.$$

Two integration formulas (MST121)

$$\int (f(x))^n f'(x)\,dx = \frac{1}{n+1}(f(x))^{n+1} + c \quad (n \neq -1)$$

$$\int \frac{f'(x)}{f(x)}\,dx = \ln(f(x)) + c \quad (f(x) > 0)$$

Modelling motion (MST121)

The SI units for kinematic quantities are as follows.

- ◇ Time is measured in seconds (s).
- ◇ Position is measured in metres (m).
- ◇ Velocity is measured in metres per second ($\mathrm{m\,s^{-1}}$).
- ◇ Acceleration is measured in metres per second per second ($\mathrm{m\,s^{-2}}$).

Time t, position s, velocity v and acceleration a are related by the equations

$$v = \frac{ds}{dt} \quad \text{and} \quad a = \frac{dv}{dt}.$$

The following formulas apply for the motion of a particle along a straight line with constant acceleration a, if at time $t = 0$ the particle has velocity v_0 and position s_0.

- ◇ The velocity v of the particle is given by

  $$v = at + v_0.$$

- ◇ The position s of the particle is given by

  $$s = \tfrac{1}{2}at^2 + v_0 t + s_0.$$

- ◇ The velocity and position of the particle are related by the equation

  $$v^2 - 2as = v_0^2 - 2as_0.$$

Finding the area under a graph (MST121–MS221)

If $f(x)$ is a continuous function that takes no negative values for $a \leq x \leq b$, then the area of the region bounded by the graph of $y = f(x)$, the x-axis, and the lines $x = a$ and $x = b$, is equal to the definite integral

$$\int_a^b f(x)\,dx.$$

In general

$$\int_a^b f(x)dx = A_1 - A_2,$$

where

- ◇ A_1 is the sum of the areas between $x = a$ and $x = b$ that are bounded below by the x-axis, and above by the graph of $y = f(x)$;
- ◇ A_2 is the sum of the areas between $x = a$ and $x = b$ that are bounded above by the x-axis, and below by the graph of $y = f(x)$.

Properties of the limits of integration (MS221)

$$\int_a^a f = 0 \qquad \int_b^a f = -\int_a^b f \qquad \int_a^b f + \int_b^c f = \int_a^c f$$

Fundamental Theorem of Calculus (MST121–MS221)

If f is a function which is continuous on the interval $[a, b]$, then it has an integral F over $[a, b]$, and

$$\int_a^b f = F(b) - F(a) = \lim_{N\to\infty}\left(\sum_{i=0}^{N-1} hf(a+ih)\right), \quad \text{where } h = \frac{b-a}{N}.$$

Integration by parts (MS221)

$$\int f(x)g'(x)\,dx = f(x)g(x) - \int f'(x)g(x)\,dx$$

$$\int_a^b f(x)g'(x)\,dx = [f(x)g(x)]_a^b - \int_a^b f'(x)g(x)\,dx$$

The integral must involve a product that can be written in the form $f\,g'$. In choosing the functions f and g, there are two guiding principles.

- ◇ Choose g' to be a function for which you can find g; that is, you must be able to integrate your chosen function g'.
- ◇ The resulting integral $\int f'\,g$, obtained by using the formula, should be simpler than the integral with which you started.

Integration by substitution (MS221)

$$\int f(g(x))g'(x)\,dx = \int f(u)\,du, \quad \text{where } u = g(x)$$

$$\int_a^b f(g(x))g'(x)\,dx = \int_{g(a)}^{g(b)} f(u)\,du, \quad \text{where } u = g(x)$$

The main steps in integration by substitution are as follows.

1. Choose $u = g(x)$ and find $\dfrac{du}{dx} = g'(x)$.
2. Substitute $u = g(x)$ into $f(g(x))$ and replace $g'(x)dx$ by du.
3. Find $\int f(u)\,du$.
4. Substitute back for u in terms of x.

Volume of solids of revolution (MS221)

If f is any function that is continuous on the interval $[a, b]$, then the volume of the solid of revolution generated by the region bounded by the graph of f from $x = a$ to $x = b$ is given by

$$\text{Volume of revolution} = \pi \int_a^b (f(x))^2\,dx.$$

MST121 Chapter C3 Differential equations and modelling

Differential equations

A **differential equation** is an equation that relates an independent variable, x say, a dependent variable, y say, and one or more derivatives of y with respect to x. The **order** of a differential equation is the order of the highest derivative that appears in the equation. A **first-order** differential equation involves the first derivative, dy/dx, and no higher derivatives.

A **solution** of a differential equation is a function $y = F(x)$ (or a more general equation relating x and y) for which the differential equation is satisfied. The **general solution** of a differential equation is the set of all possible solutions of the equation. It usually involves one or more arbitrary constants. A **particular solution** of a differential equation is a single solution of the equation, which consists of a relationship between the dependent and independent variables that contains no arbitrary constant.

An **initial condition** associated with a first-order differential equation requires that the dependent variable y takes a specified value, b say, when the independent variable x has a given value, a say. This is often written as

$$y = b \text{ when } x = a, \quad \text{or as} \quad y(a) = b.$$

The numbers a and b are called **initial values** for x and y, respectively. The combination of a first-order differential equation and an initial condition is called an **initial-value problem**. The solution of an initial-value problem is a particular solution of the differential equation which also satisfies the initial condition.

Direct integration

The general solution of the differential equation $dy/dx = f(x)$ is the indefinite integral

$$y = \int f(x)\,dx = F(x) + c,$$

where $F(x)$ is any integral of $f(x)$ and c is an arbitrary constant. Any initial condition

$$y = b \text{ when } x = a, \quad \text{that is,} \quad y(a) = b,$$

enables a value for the arbitrary constant c to be found. The corresponding particular solution satisfies both the differential equation and the initial condition.

Implicit differentiation

If y is a function of x and $H(y) = F(x)$, then $H'(y)\dfrac{dy}{dx} = F'(x)$.

Separation of variables

The method applies to differential equations of the form $dy/dx = f(x)g(y)$.

1. Divide both sides by $g(y)$, for $g(y) \neq 0$, to obtain

$$\frac{1}{g(y)}\frac{dy}{dx} = f(x).$$

2. Integrate both sides with respect to x. The outcome is

$$\int \frac{1}{g(y)}\,dy = \int f(x)\,dx.$$

3. Carry out the two integrations, introducing *one* arbitrary constant, to obtain the general solution in implicit form. If possible, manipulate the resulting equation to make y the subject, thus expressing the general solution in explicit form.

Modelling growth and decay

The differential equation $dy/dx = Ky$, where K is a constant, has the general solution $y = Ae^{Kx}$, where A is an arbitrary constant.

The process of radioactive decay, that is, the change in mass m of a radioactive substance that is present at time t, can be modelled by the initial-value problem

$$\frac{dm}{dt} = -km \quad (m > 0), \quad m = m_0 \text{ when } t = 0.$$

Here k is a positive constant, called the **decay constant**, and m_0 is the initial mass of the substance. This initial-value problem has the solution

$$m = m_0 e^{-kt}.$$

The **half-life** T of a radioactive substance is the time it takes for the mass of radioactive substance to diminish to half its original amount. In the model, it is given by $T = (\ln 2)/k$. The value of the decay constant k can be estimated from data by plotting $\ln(m/m_0)$ against time t. This should approximate a line through the origin with gradient $-k$.

The process of population change, that is, the change in the population size P over time t, can be modelled by the initial-value problem

$$\frac{dP}{dt} = KP \quad (P > 0), \quad P = P_0 \text{ when } t = 0.$$

Here K is a constant, called the **proportionate growth rate**, and P_0 is the initial population size. This initial-value problem has the solution

$$P = P_0 e^{Kt}.$$

If $K < 0$ then the population is decreasing and the half-life of the population can be defined as for radioactive decay. If $K > 0$ then the population is increasing and the **doubling time** T of the population is the time it takes for the population to double in size. In the model, it is given by $T = (\ln 2)/K$. The value of the proportionate growth rate K can be estimated from data using a log-linear plot of $\ln P$ against t. This should approximate a line which crosses the $(\ln P)$-axis at $\ln P_0$ and has gradient K.

Euler's method

Euler's method for solving the initial-value problem

$$\frac{dy}{dx} = f(x, y), \quad y(x_0) = y_0$$

is described by the pair of recurrence relations

$$x_{n+1} = x_n + h, \quad y_{n+1} = y_n + hf(x_n, y_n) \quad (n = 0, 1, 2, \ldots),$$

where h is the step size between the successive values of x at which solution estimates are calculated. Each calculated value y_n is an estimate of the corresponding 'true solution' y at $x = x_n$; that is, y_n is an estimate of $y(x_n)$. The sequence of estimates depends on the choice of both the step size h and the overall number of steps N. Decreasing h, while increasing N to cover the same range of x-values, leads to progressively improved estimates for the solution values, and with a small enough step size, any desired level of accuracy can be achieved.

MS221 Chapter C3 Taylor polynomials

Taylor polynomials of degree n

Let f be a function that is n-times differentiable at 0. The **Taylor polynomial** of degree n about 0 for f is

$$p(x) = f(0) + f'(0)x + \frac{f''(0)}{2!}x^2 + \frac{f^{(3)}(0)}{3!}x^3 + \cdots + \frac{f^{(n)}(0)}{n!}x^n.$$

The **Taylor polynomial** of degree n about a for f is

$$p(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \frac{f^{(3)}(a)}{3!}(x-a)^3 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n.$$

A Taylor polynomial of degree n may be denoted by $p_n(x)$.

Approximating function values using Taylor polynomials

To obtain an approximation to a function value that is accurate to m decimal places, calculate approximations using Taylor polynomials of degree 1, 2, 3, and so on, until two successive approximations agree to $m + 2$ decimal places. Note that for odd (or even) functions, this rule of thumb should be applied to the Taylor polynomials about 0 of odd (or even) degree.

Taylor series about a

Let f be a function that is differentiable infinitely many times at a. The **Taylor series** about a for f is

$$f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \frac{f^{(3)}(a)}{3!}(x-a)^3 + \cdots + \frac{f^{(k)}(a)}{k!}(x-a)^k + \cdots.$$

The point a is called the **centre** of the Taylor series. If $a = 0$, then the Taylor series reduces to

$$f(0) + f'(0)x + \frac{f''(0)}{2!}x^2 + \frac{f^{(3)}(0)}{3!}x^3 + \cdots + \frac{f^{(k)}(0)}{k!}x^k + \cdots.$$

Any range of values of x for which a Taylor series for a function f sums to $f(x)$ is called a **range of validity** for the series.

Standard Taylor series about 0

$$\begin{aligned}
\sin x &= x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5 - \frac{1}{7!}x^7 + \frac{1}{9!}x^9 - \cdots, \quad \text{for } x \in \mathbb{R} \\
\cos x &= 1 - \frac{1}{2!}x^2 + \frac{1}{4!}x^4 - \frac{1}{6!}x^6 + \frac{1}{8!}x^8 - \cdots, \quad \text{for } x \in \mathbb{R} \\
e^x &= 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \frac{1}{4!}x^4 + \cdots, \quad \text{for } x \in \mathbb{R} \\
\ln(1+x) &= x - \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 - \tfrac{1}{4}x^4 + \tfrac{1}{5}x^5 - \cdots, \quad \text{for } -1 < x < 1 \\
\frac{1}{1-x} &= 1 + x + x^2 + x^3 + x^4 + \cdots, \quad \text{for } -1 < x < 1 \\
(1+x)^\alpha &= 1 + \alpha x + \frac{\alpha(\alpha-1)}{2!}x^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{3!}x^3 + \cdots, \\
&\qquad \text{for } -1 < x < 1, \text{ where } \alpha \in \mathbb{R}
\end{aligned}$$

Manipulating Taylor series

New Taylor series can be obtained from standard Taylor series by:

- ◇ substituting for the variable;
- ◇ adding, subtracting and multiplying Taylor series;
- ◇ differentiating and integrating Taylor series term by term.

In each case, a range of validity of the new Taylor series can be found from the known range(s) of validity of the standard Taylor series involved.

For example, the hyperbolic sine and cosine functions,

$$\sinh x = \tfrac{1}{2}(e^x - e^{-x}) \quad \text{and} \quad \cosh x = \tfrac{1}{2}(e^x + e^{-x}),$$

have Taylor series

$$\sinh x = x + \frac{1}{3!}x^3 + \frac{1}{5!}x^5 + \cdots, \quad \text{for } x \in \mathbb{R},$$

and

$$\cosh x = 1 + \frac{1}{2!}x^2 + \frac{1}{4!}x^4 + \cdots, \quad \text{for } x \in \mathbb{R}.$$

MST121 Chapter D1 Chance

Probability

For any event E, $0 \leq P(E) \leq 1$.

If an event E never happens, then $P(E) = 0$.

If an event E is certain to happen, then $P(E) = 1$.

If an experiment has N equally-likely possible outcomes, and $n(E)$ is the number of these outcomes that give rise to an event E, then

$$P(E) = \frac{n(E)}{N};$$

that is, $P(E)$ is equal to the number of outcomes for which the event E occurs divided by the total number of possible outcomes.

If E is an event and not-E is the opposite event (that E does not occur), then

$$P(E) + P(\text{not-}E) = 1,$$

or, equivalently,

$$P(E) = 1 - P(\text{not-}E).$$

Two events are **independent** of each other if the occurrence (or not) of one is not influenced by whether or not the other occurs.

The **multiplication rule for independent events** states that if E and F are independent events, then

$$P(E \text{ and } F) = P(E) \times P(F).$$

Geometric distributions

If a sequence of trials of an experiment is carried out and the probability of success in each trial is p $(0 < p < 1)$ independently of the results of earlier trials, then X, the number of trials required to obtain a success, has a **geometric distribution**. The probability function of X is given by

$$P(X = j) = (1 - p)^{j-1}p, \quad j = 1, 2, 3, \ldots.$$

The mean number of trials required to obtain a success is $1/p$.

Probability distributions

The **mean** of the probability distribution of a discrete random variable X is denoted by μ and is defined to be

$$\mu = \sum_j j \times P(X = j),$$

where the summation is over all values j which X can take, that is, for which $P(X = j) > 0$.

The corresponding formula for the mean of a continuous random variable X with probability density function f is

$$\mu = \int_{-\infty}^{\infty} x\, f(x)\, dx.$$

MST121 Chapter D2 Modelling variation

The **variance** of a random variable X or of a probability distribution is the mean of the values $(x - \mu)^2$, where the mean is taken over all values x that X can take. The **standard deviation** of a random variable or of a probability distribution is the square root of the variance.

When a probability distribution is used to model the variation in a population, the mean of the distribution is called the **population mean**, and the standard deviation is called the **population standard deviation**. The population mean and the population standard deviation are examples of **population parameters**.

Sample statistics and population parameters

For a sample of n observations $x_1, x_2, \ldots, x_n$, the **sample mean** $\overline{x}$ is given by

$$\overline{x} = \frac{1}{n}(x_1 + x_2 + \cdots + x_n) = \frac{1}{n}\sum_{i=1}^{n} x_i,$$

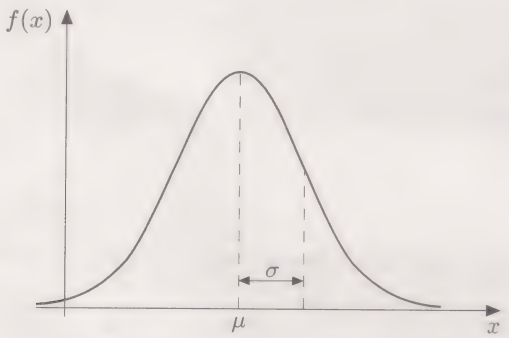
and the **sample standard deviation** s is given by

$$s = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2}.$$

The sample mean and sample standard deviation are examples of **sample statistics**. In general, given a sample of data from a population, the sample mean $\overline{x}$ is used to estimate the population mean μ, and the sample standard deviation s is used to estimate the population standard deviation σ.

Normal distributions

A **normal distribution** is a continuous probability distribution. Probabilities are calculated by finding areas under a normal curve, which has the following typical shape.



The probability density function of a normal distribution is the function f, where $y = f(x)$ is the equation of the normal curve. It is defined for all real values of x. The equation of a normal curve contains two parameters, μ and σ: μ is the mean of the distribution, and σ is its standard deviation. The curve is symmetric about its peak, which occurs at $x = \mu$. The normal distribution with mean 0 and standard deviation 1 is called the **standard normal distribution**.

If a normal distribution is used to model the variation in a population, then, according to the model, the proportion of the population within k standard deviations of the mean is the same whatever the values of the mean μ and the standard deviation σ. In particular, approximately 95% of the population are within 1.96 standard deviations of the mean (that is, between $\mu - 1.96\sigma$ and $\mu + 1.96\sigma$).

MST121 Chapter D3 Estimating

Sampling distributions, the Central Limit Theorem and confidence intervals

The sampling distribution of the mean for samples of size n from a population with mean μ and standard deviation σ has mean μ and standard deviation $\sigma/\sqrt{n}$. These results hold for any sample size.

The standard deviation of the sampling distribution of the mean is called the **standard error of the mean** and is denoted by SE.

The **Central Limit Theorem** states that, for large sample sizes (at least 25), the sampling distribution of the mean for samples of size n from a population with mean μ and standard deviation σ may be approximated by a normal distribution with mean μ and standard deviation

$$SE = \frac{\sigma}{\sqrt{n}}.$$

Given a sample of size n from a population, a **95% confidence interval** for the population mean μ is given by

$$\left(\overline{x} - 1.96\frac{s}{\sqrt{n}},\ \overline{x} + 1.96\frac{s}{\sqrt{n}}\right),$$

where $\overline{x}$ is the sample mean and s is the sample standard deviation. The sample size n must be at least 25.

MST121 Chapter D4 Further investigations

Summary statistics and boxplots

The **median** is essentially the middle value of a batch of data when the values are placed in order of increasing size. If the batch size is odd, then the median is the middle value. If the batch size is even, then the median is the mean of the middle two values.

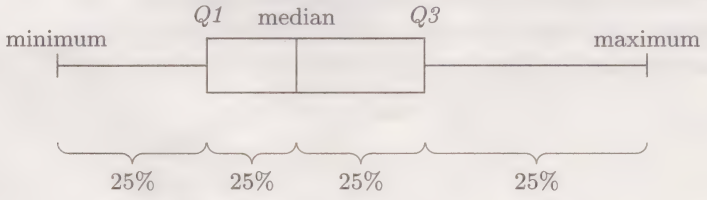
The **lower quartile**, which is denoted by $Q1$, is the median of the values to the left of the median.

The **upper quartile**, which is denoted by $Q3$, is the median of the values to the right of the median.

The **interquartile range** is the difference between the upper quartile and the lower quartile.

The **range** is the difference between the maximum value and the minimum value.

A **boxplot** is a diagram for representing a batch of data. A typical boxplot is shown below.



The box extends from the lower quartile to the upper quartile, and a vertical line is drawn through the box at the median. The whiskers extend from the ends of the box to the minimum and maximum values in the batch of data.

Hypothesis testing

There are three stages involved in a hypothesis test:

1. Set up the null and alternative hypotheses.
2. Calculate the test statistic.
3. Report conclusions.

The **two-sample z-test** is a hypothesis test which may be used when a sample of at least 25 observations is available from each of two populations. It may be used to investigate whether there is a difference between the means of the populations. The three stages involved in carrying out the two-sample z-test are outlined below.

Stage 1: Hypotheses

Set up the null and alternative hypotheses:

$$H_0 : \mu_A = \mu_B,$$
$$H_1 : \mu_A \neq \mu_B,$$

where μ_A and μ_B are the means of populations A and B, respectively.

Stage 2: The test statistic

Calculate the test statistic

$$z = \frac{\overline{x}_A - \overline{x}_B}{ESE},$$

where

$$ESE = \sqrt{\frac{s_A^2}{n_A} + \frac{s_B^2}{n_B}},$$

$\overline{x}_A$ and $\overline{x}_B$ are the sample means, s_A and s_B are the sample standard deviations, and n_A and n_B are the sizes of the samples from A and B, respectively.

Stage 3: Conclusions

- ◇ If $z \leq -1.96$ or $z \geq 1.96$, then H_0 is rejected at the 5% significance level in favour of the alternative hypothesis.
- ◇ If $-1.96 < z < 1.96$, then H_0 is not rejected at the 5% significance level.

The conclusion should be expressed in terms of the hypothesis being tested.

The quantity ESE in the test statistic for the two-sample z-test is the estimated standard error of the difference between two sample means; that is, it is the estimated value of the standard deviation of the sampling distribution of the difference between two sample means.

Fitting lines to data

The **least squares fit line** for a set of data points is the line that minimises the sum of the squared residuals for the data set. It is also known as the **regression line** of y on x. It may be used to predict values of y, the **dependent variable**, for values of x, the **explanatory variable**, but not vice versa. It should be used only to predict y-values for x-values that are within, or just outside, the range of values of x represented in the data.

MS221 Chapter D1 Complex numbers

Arithmetic of complex numbers

For complex numbers $z = a + bi$ and $w = c + di$, the following properties hold.

Equality	$z = w$ if and only if $a = c$ and $b = d$.
Conjugate	$\overline{z} = a - bi$.
Modulus	$\lvert z\rvert = \sqrt{a^2 + b^2} = \lvert\overline{z}\rvert$.
Addition	$z + w = (a + c) + (b + d)i$.
Subtraction	$z - w = (a - c) + (b - d)i$.
Multiplication	$z \times w = (ac - bd) + (ad + bc)i$.
Reciprocal	$\dfrac{1}{z} = z^{-1} = \dfrac{a - bi}{a^2 + b^2} = \dfrac{\overline{z}}{\lvert z\rvert^2}$ (where $z \neq 0$).
Division	$\dfrac{w}{z} = wz^{-1} = \dfrac{w \times \overline{z}}{z \times \overline{z}} = \dfrac{w \times \overline{z}}{\lvert z\rvert^2}$ (where $z \neq 0$).
Exponentials	$e^{a+bi} = e^a(\cos b + i \sin b)$.

Operations in polar form

For complex numbers $\langle r, \theta\rangle$ and $\langle s, \phi\rangle$ in polar form, the following properties hold.

Equality	$\langle r, \theta\rangle = \langle s, \phi\rangle$ if and only if $r = s$ and $\theta - \phi = 2m\pi$, where $m \in \mathbb{Z}$.
Conjugate	The conjugate of $\langle r, \theta\rangle$ is $\langle r, -\theta\rangle$.
Multiplication	$\langle r, \theta\rangle \times \langle s, \phi\rangle = \langle rs, \theta + \phi\rangle$.
Powers	$\langle r, \theta\rangle^n = \langle r^n, n\theta\rangle$.

Exponential form

The **argument** of $z = re^{i\theta}$ is $\arg(z) = \theta$. The **principal value** of $\arg(z)$ lies in the interval $(-\pi, \pi]$. The conjugate of $z = re^{i\theta}$ is $\overline{z} = re^{-i\theta}$.

Transforming complex numbers into alternative representations

Polar form to Cartesian form:

$$\langle r, \theta\rangle = r(\cos\theta + i \sin\theta).$$

Cartesian form to polar form:

$$z = a + bi = \langle r, \theta\rangle, \quad \text{where } r = \lvert z\rvert = \sqrt{a^2 + b^2} \text{ and } \theta \text{ is an argument of } z.$$

Note that
$\cos\theta = a/r$
and
$\sin\theta = b/r$.

Polar form to exponential form and vice versa:

$$\langle r, \theta\rangle = re^{i\theta}.$$

Exponential form to Cartesian form:

$$re^{i\theta} = r(\cos\theta + i \sin\theta).$$

Cartesian form to exponential form:

$$z = a + bi = re^{i\theta}, \quad \text{where } r = \lvert z\rvert = \sqrt{a^2 + b^2} \text{ and } \theta \text{ is an argument of } z.$$

Polynomials and roots

A **root** of a polynomial $p(z)$ is a solution of $p(z) = 0$. The number α is a root of $p(z)$ if and only if $(z - \alpha)$ is a factor of $p(z)$; that is, $p(z) = (z - \alpha)q(z)$, where $q(z)$ is another polynomial.

Any polynomial $p(z)$ of degree n can be factorised into n linear factors:

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = a_n(z - \alpha_1)(z - \alpha_2) \cdots (z - \alpha_n) \quad (a_n \neq 0).$$

In general, the roots α_i are complex and may include repetitions.

The n roots of the equation $z^n = 1$ are called **nth roots of unity**.

If $p(z)$ is a polynomial with real coefficients, and α is a complex root of $p(z)$, then $\overline{\alpha}$ is also a root of $p(z)$.

Finding roots

To solve the equation $z^n = a$ and so find the nth roots of a.

1. Represent z in polar form as $\langle r, \theta \rangle$ and a in polar form as $\langle s, \phi \rangle$.
2. Then $z^n = a$ can be written as $\langle r, \theta \rangle^n = \langle s, \phi \rangle$; that is, as $\langle r^n, n\theta \rangle = \langle s, \phi \rangle$.
3. Hence $r^n = s$ and $n\theta = \phi + 2m\pi$, where $m \in \mathbb{Z}$.
4. Since r and s are real and positive, there is only one solution r to $r^n = s$.
5. Calculate $\theta = (\phi + 2m\pi)/n$, for $m = 0, 1, 2, \ldots, n - 1$.
6. The n values of $\langle r, \theta \rangle$ are the nth roots of a; they are regularly spaced around a circle centred at 0.

Complex recurrences

The recurrence

$$c_0 = 1, \quad c_{n+1} = kc_n \quad (n = 0, 1, 2, \ldots),$$

where k is a complex number, has the closed form $c_n = k^n$ $(n = 0, 1, 2, \ldots)$. The sequence generated by this recurrence has the following properties.

- ◇ The sequence repeats itself if and only if k is a root of unity.
- ◇ If $|k| = 1$, then the points of the sequence all lie on the unit circle on an Argand diagram.
- ◇ If $|k| > 1$, then the points of the sequence lie on an expanding spiral on an Argand diagram.
- ◇ If $|k| < 1$, then the points of the sequence lie on a contracting spiral on an Argand diagram.

Continuous spirals

For $a > 0$, plotting the image of the complex-valued function $f(t) = a^t e^{it}$ $(t \geq 0)$ on an Argand diagram gives

- ◇ a circle if $a = 1$;
- ◇ a continuous expanding spiral if $a > 1$;
- ◇ a continuous contracting spiral if $0 < a < 1$.

MS221 Chapter D2 Number theory

Division Algorithm

Let a and n be integers, with n positive. Then there are unique integers q and r such that

$$a = qn + r, \quad (\text{where } 0 \leq r < n).$$

The number q is the **quotient** and r is the **remainder** on division of a by n.
If $r = 0$, then a is **divisible** by n, and n is a **factor**, or **divisor**, of a.

Congruences

Let n be a positive integer. Two integers a and b are **congruent modulo** n if $a - b$ is a multiple of n, that is, if a and b have the same remainder on division by n. This is written as a **congruence**,

$$a \equiv b \pmod{n},$$

and n is called the **modulus** of the congruence.

Properties of congruences

Let n and k be positive integers, and a, b, c, d be integers. Then the following hold.

(a) $a \equiv a \pmod{n}$.
(b) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
(c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.
(e) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.
(f) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

Repeated squaring

A congruence for a high power can be found efficiently by repeated squaring. For example, to find the remainder of 14^{27} on division by 55, first calculate:

$$14^1 \equiv 14 \pmod{55},$$
$$14^2 = 196 \equiv 31 \pmod{55},$$
$$14^4 = (14^2)^2 \equiv 31^2 \equiv 961 \equiv 26 \pmod{55},$$
$$14^8 = (14^4)^2 \equiv 26^2 \equiv 676 \equiv 16 \pmod{55},$$
$$14^{16} = (14^8)^2 \equiv 16^2 \equiv 256 \equiv 36 \pmod{55}.$$

Since $27 = 1 + 2 + 8 + 16$, we obtain

$$\begin{aligned} 14^{27} &= 14^1 \times 14^2 \times 14^8 \times 14^{16} \\ &\equiv 14 \times 31 \times 16 \times 36 \pmod{55} \\ &\equiv 249\,984 \pmod{55} \\ &\equiv 9 \pmod{55}. \end{aligned}$$

Divisibility tests

A number is divisible by 2 if and only if its final digit is divisible by 2.

A number is divisible by 3 if and only if its digit sum is divisible by 3.

A number is divisible by 4 if and only if the number comprising its final two digits is divisible by 4.

A number is divisible by 5 if and only if its final digit is 5 or 0.

A number is divisible by 6 if and only if it is divisible by both 2 and 3.

A number is divisible by 8 if and only if the number comprising its final three digits is divisible by 8.

A number is divisible by 9 if and only if its digit sum is divisible by 9.

A number is divisible by 10 if and only if its final digit is 0.

A number is divisible by 11 if and only if its alternating digit sum is divisible by 11.

A number is divisible by 12 if and only if it is divisible by both 3 and 4.

To test a number a for divisibility by 7 (or 13):

split a every three digits starting from the right;
find the remainder of each 3-digit number on division by 7 (or 13):
form the alternating sum of these remainders.

The resulting number will be congruent to a modulo 7 (or 13).

Modular arithmetic

For a and b in $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$:

- $a +_n b$ is the remainder on division of $a + b$ by n;
- $a \times_n b$ is the remainder on division of $a \times b$ by n.

The operations $+_n$ and $\times_n$ are both commutative and associative on the set $\mathbb{Z}_n$.

Multiplicative inverses

Two positive integers a and b have a **common factor** c if c is a factor of both a and b.

If the only common factor of a and b is $c = 1$, then a and b are **coprime**.

Let n, a and b be positive integers, with a and b in $\mathbb{Z}_n$, and suppose that $a \times_n b = 1$. Then b is the **multiplicative inverse** of a in $\mathbb{Z}_n$.

Let n and a be positive integers, with a in $\mathbb{Z}_n$. The following three statements are equivalent:

(a) a and n are coprime;

(b) a has a multiplicative inverse in $\mathbb{Z}_n$;

(c) row a of the multiplication table for $\mathbb{Z}_n$ includes all of $\mathbb{Z}_n$.

In particular, if p is a prime number, then each non-zero row of the multiplication table for $\mathbb{Z}_p$ includes all of $\mathbb{Z}_p$ and each non-zero a in $\mathbb{Z}_p$ has a multiplicative inverse in $\mathbb{Z}_p$.

Euclid's Algorithm

Euclid's Algorithm provides a method for finding the multiplicative inverse of a number a in $\mathbb{Z}_n$, when it exists. Here it is illustrated with $a = 9$, $n = 25$; the aim is to find b in $\mathbb{Z}_{25}$ such that $9 \times_{25} b = 1$.

1. Apply the Division Algorithm repeatedly:

$$25 = 2 \times 9 + 7 \quad \text{(dividing 25 by 9)},$$
$$9 = 1 \times 7 + 2 \quad \text{(dividing 9 by 7)},$$
$$7 = 3 \times 2 + 1 \quad \text{(dividing 7 by 2)}. \qquad (*)$$

2. Work backwards from $(*)$, to obtain

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ &= 7 - 3(9 - 1 \times 7) \\ &= -3 \times 9 + 4 \times 7 \\ &= -3 \times 9 + 4(25 - 2 \times 9) \\ &= 4 \times 25 - 11 \times 9. \end{aligned}$$

   Thus $9 \times (-11) \equiv 1 \pmod{25}$.

3. Since $-11 \equiv 14 \pmod{25}$, we deduce that

$$9 \times 14 \equiv 1 \pmod{25}.$$

   Hence $b = 14$ is the multiplicative inverse of 9 in $\mathbb{Z}_{25}$.

Fermat's Little Theorem

Let p be a prime number, and let a be a positive integer that is not a multiple of p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat's Little Theorem can be used to find remainders of high powers modulo p.

Here it is used to find the remainder when 16^{103} is divided by 11.

1. Since $16 \equiv 5 \pmod{11}$, we have $16^{103} \equiv 5^{103} \pmod{11}$.
2. By Fermat's Little Theorem with $p = 11$ and $a = 5$, we know that

$$5^{10} \equiv 1 \pmod{11}.$$

3. Therefore

$$16^{103} \equiv 5^{103} \equiv (5^{10})^{10} \times 5^3 \equiv 1 \times 125 \equiv 4 \pmod{11}.$$

   Hence the remainder when 16^{103} is divided by 11 is 4.

Cryptography

A **cipher** is a one-one function f with domain Ω and codomain Ω, where Ω is a finite set of characters. It is applied to encipher **messagetext** (a **message**) by transforming it into **ciphertext**.

The inverse function f^{-1} of f has domain Ω and is used to decipher ciphertext by transforming it into the corresponding messagetext.

Additive ciphers

Let n be a positive integer, and let k be in $\mathbb{Z}_n$ with $k \neq 0$. The **additive cipher** A_k on $\mathbb{Z}_n$ has rule

$$A_k(m) = m +_n k.$$

The inverse function A_k^{-1} has rule

$$A_k^{-1}(c) = c +_n k',$$

where k' is the additive inverse of k in $\mathbb{Z}_n$.

For example, in $\mathbb{Z}_{26}$, the additive cipher A_3 enciphers 2 to $A_3(2) = 2 +_{26} 3 = 5$, and A_3 has inverse function $A_3^{-1} = A_{23}$, since $3 + 23 = 26$.

Multiplicative ciphers

Let n be a positive integer, and let k in $\mathbb{Z}_n$ be coprime with n. The **multiplicative cipher** M_k on $\mathbb{Z}_n$ has rule

$$M_k(m) = k \times_n m.$$

The inverse function M_k^{-1} has rule

$$M_k^{-1}(c) = k' \times_n c,$$

where k' is the multiplicative inverse of k in $\mathbb{Z}_n$.

For example, in $\mathbb{Z}_{26}$, the multiplicative cipher M_3 enciphers 2 to $M_3(2) = 2 \times_{26} 3 = 6$, and M_3 has inverse function $M_3^{-1} = M_9$, since $3 \times_{26} 9 = 1$.

Exponential ciphers

Let p be a prime number, and let k in $\mathbb{Z}_{p-1}$ be coprime with $p - 1$. The **exponential cipher** E_k on $\mathbb{Z}_p$ has rule

$$E_k(m) \equiv m^k \pmod{p}.$$

The inverse function E_k^{-1} has rule

$$E_k^{-1}(c) \equiv c^{k'} \pmod{p},$$

where k' is the multiplicative inverse of k in $\mathbb{Z}_{p-1}$.

For example, in $\mathbb{Z}_{29}$, the exponential cipher E_3 enciphers 2 to $E_3(2) = 2^3 = 8$, and E_3 has inverse function $E_3^{-1} = E_{19}$, since $3 \times_{28} 19 = 1$.

RSA ciphers

Let p and q be prime numbers, and let k in $\mathbb{Z}_{(p-1)(q-1)}$ be coprime with $(p-1)(q-1)$. The **RSA cipher** R_k on $\mathbb{Z}_{pq}$ has rule

$$R_k(m) \equiv m^k \pmod{pq}.$$

The inverse function R_k^{-1} has rule

$$R_k^{-1}(c) \equiv c^{k'} \pmod{pq},$$

where k' is the multiplicative inverse of k in $\mathbb{Z}_{(p-1)(q-1)}$.

For example, in $\mathbb{Z}_{55}$, the RSA cipher R_3 enciphers 2 to $R_3(2) = 2^3 = 8$, and R_3 has inverse function $R_3^{-1} = R_{27}$, since $3 \times_{40} 27 = 1$ (if $p = 5$ and $q = 11$, then $(p-1)(q-1) = 40$).

MS221 Chapter D3 Groups

Symmetries

A **symmetry** of a plane set X is a (plane) isometry that maps the set X to itself. Symmetries have the following properties.

- ◇ The set of symmetries $S(X)$ of a plane set X is **closed** under the operation of composition; that is, for all $f, g \in S(X)$,

  $$g \circ f \in S(X).$$

- ◇ The set of symmetries $S(X)$ of a plane set X contains the **identity** symmetry e, with the property that, for all $f \in S(X)$,

  $$f \circ e = f = e \circ f.$$

- ◇ Each symmetry f in $S(X)$ has an **inverse** symmetry f^{-1} in $S(X)$ with the property that

  $$f \circ f^{-1} = e = f^{-1} \circ f.$$

- ◇ Composition of symmetries is **associative**; that is, for all $f, g, h \in S(X)$,

  $$h \circ (g \circ f) = (h \circ g) \circ f.$$

In particular, rotations r_θ, $0 \leq \theta < 2\pi$, and reflections q_ϕ, $0 \leq \phi < \pi$, have the following properties.

$\circ$	r_θ	q_θ
r_ϕ	$r_{\phi+\theta \pmod{2\pi}}$	$q_{\frac{1}{2}\phi+\theta \pmod{\pi}}$
q_ϕ	$q_{\phi-\frac{1}{2}\theta \pmod{\pi}}$	$r_{2\phi-2\theta \pmod{2\pi}}$

$$r_0^{-1} = r_0,$$
$$r_\theta^{-1} = r_{2\pi-\theta} \quad (0 < \theta < 2\pi),$$
$$q_\phi^{-1} = q_\phi \quad (0 < \phi < \pi).$$

Groups and their properties

Let G be a set, and let $*$ be a binary operation on G. Then $(G, *)$ is a group if the following four properties hold.

G1	Closure	For all $g, h \in G$, $g * h \in G$.
G2	Identity	There exists an identity element $e \in G$ such that, for all $g \in G$, $g * e = g = e * g$.
G3	Inverses	For all $g \in G$, there exists an inverse element $g^{-1} \in G$ such that $g * g^{-1} = e = g^{-1} * g$.
G4	Associativity	For all $g, h, k \in G$, $g * (h * k) = (g * h) * k$.

In any group, the identity element is unique and the inverse of each element is unique.

The **order** of a group is the number of elements in the group. For a finite group $(G, *)$, the effect of the binary operation $*$ can be shown in a **Cayley table**. In a Cayley table, each element of the group appears exactly once in each row and exactly once in each column.

A group $(G, *)$ is called **Abelian** if it is commutative; that is, for all $g, h \in G$,

$$g * h = h * g.$$

Examples of groups

- ◇ The set $S(X)$ of symmetries of a plane set X forms the **symmetry group** of X under the operation $\circ$.
- ◇ For each $n \geq 2$, $\mathbb{Z}_n$ is an Abelian group under $+_n$.
- ◇ For each prime number p, $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ is an Abelian group under $\times_p$.

Cayley tables for selected groups

In the Cayley tables for symmetry groups, the isometry in the top border is performed first, followed by the isometry in the left border. For example, in the Cayley table for $(S(\triangle), \circ)$, we have $q_{\pi/2} \circ r_{2\pi/3} = q_{\pi/6}$.

For all $n \in \mathbb{N}$, the Cayley table for $(\mathbb{Z}_n, +_n)$ has the 'constant diagonal' pattern.

Cayley table for $(\mathbb{Z}_4, +_4)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Cayley table for $(S(\rhd), \circ)$

$\circ$	e	r_π	q_0	$q_{\pi/2}$
e	e	r_π	q_0	$q_{\pi/2}$
r_π	r_π	e	$q_{\pi/2}$	q_0
q_0	q_0	$q_{\pi/2}$	e	r_π
$q_{\pi/2}$	$q_{\pi/2}$	q_0	r_π	e

Cayley table for $(\mathbb{Z}_6, +_6)$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Cayley table for $(S(\triangle), \circ)$

$\circ$	e	$r_{2\pi/3}$	$r_{4\pi/3}$	$q_{\pi/6}$	$q_{\pi/2}$	$q_{5\pi/6}$
e	e	$r_{2\pi/3}$	$r_{4\pi/3}$	$q_{\pi/6}$	$q_{\pi/2}$	$q_{5\pi/6}$
$r_{2\pi/3}$	$r_{2\pi/3}$	$r_{4\pi/3}$	e	$q_{\pi/2}$	$q_{5\pi/6}$	$q_{\pi/6}$
$r_{4\pi/3}$	$r_{4\pi/3}$	e	$r_{2\pi/3}$	$q_{5\pi/6}$	$q_{\pi/6}$	$q_{\pi/2}$
$q_{\pi/6}$	$q_{\pi/6}$	$q_{5\pi/6}$	$q_{\pi/2}$	e	$r_{4\pi/3}$	$r_{2\pi/3}$
$q_{\pi/2}$	$q_{\pi/2}$	$q_{\pi/6}$	$q_{5\pi/6}$	$r_{2\pi/3}$	e	$r_{4\pi/3}$
$q_{5\pi/6}$	$q_{5\pi/6}$	$q_{\pi/2}$	$q_{\pi/6}$	$r_{4\pi/3}$	$r_{2\pi/3}$	e

Cayley table for $(S(\square), \circ)$

$\circ$	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$
e	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$
$r_{\pi/2}$	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	e	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$	q_0
r_π	r_π	$r_{3\pi/2}$	e	$r_{\pi/2}$	$q_{\pi/2}$	$q_{3\pi/4}$	q_0	$q_{\pi/4}$
$r_{3\pi/2}$	$r_{3\pi/2}$	e	$r_{\pi/2}$	r_π	$q_{3\pi/4}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$
q_0	q_0	$q_{3\pi/4}$	$q_{\pi/2}$	$q_{\pi/4}$	e	$r_{3\pi/2}$	r_π	$r_{\pi/2}$
$q_{\pi/4}$	$q_{\pi/4}$	q_0	$q_{3\pi/4}$	$q_{\pi/2}$	$r_{\pi/2}$	e	$r_{3\pi/2}$	r_π
$q_{\pi/2}$	$q_{\pi/2}$	$q_{\pi/4}$	q_0	$q_{3\pi/4}$	r_π	$r_{\pi/2}$	e	$r_{3\pi/2}$
$q_{3\pi/4}$	$q_{3\pi/4}$	$q_{\pi/2}$	$q_{\pi/4}$	q_0	$r_{3\pi/2}$	r_π	$r_{\pi/2}$	e

Selected infinite groups

Each of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ forms an infinite group under addition.

Each of $\mathbb{Q}^*$, $\mathbb{R}^*$ and $\mathbb{C}^*$ forms an infinite group under multiplication.

Isomorphic groups and their properties

An **isomorphism** is a one-one function from one finite group $(G, *)$ onto another finite group $(H, \diamond)$, which converts the Cayley table for $(G, *)$ to the Cayley table for $(H, \diamond)$. The two groups $(G, *)$ and $(H, \diamond)$ are **isomorphic** to each other.

Let $(G, *)$ and $(H, \diamond)$ be finite groups that are isomorphic to each other. Then:

- $|G| = |H|$;
- G and H have the same number of self-inverse elements;
- G is Abelian if and only if H is Abelian.

Groups of order up to 8

Any group of order up to 8 is isomorphic to one of the groups in the table below.

Group	Order	Self-inverses	Abelian
$(\{e\}, *)$	1	1	✓
$(\mathbb{Z}_2, +_2)$	2	2	✓
$(\mathbb{Z}_3, +_3)$	3	1	✓
$(\mathbb{Z}_4, +_4)$	4	2	✓
$(S(\square), \circ)$	4	4	✓
$(\mathbb{Z}_5, +_5)$	5	1	✓
$(\mathbb{Z}_6, +_6)$	6	2	✓
$(S(\triangle), \circ)$	6	4	×
$(\mathbb{Z}_7, +_7)$	7	1	✓
$(\mathbb{Z}_8, +_8)$	8	2	✓
$(S(\square), \circ)$	8	6	×
$(S(\text{BOX}), \circ)$	8	8	✓
$(S(\text{ROTOR}), \circ)$	8	4	✓
$(QUAT, \times)$	8	2	×

MS221 Chapter D4 Proof and reasoning

Operations combining propositions

For two propositions p and q:

- $p \wedge q$ is interpreted as 'p and q';
- $p \vee q$ is interpreted as 'either p or q or both p and q';
- $p \Rightarrow q$ is interpreted as 'if p then q' or, equivalently, as 'p implies q';
- $p \Leftrightarrow q$ is interpreted as 'p if and only if q', so $p \Leftrightarrow q$ means $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

Truth values

The truth value of a **simple proposition** derives from knowledge of the content of that proposition. The truth value of a **compound proposition** depends on the truth or falsity of the propositions being combined, and can be derived from the truth tables of the operations involved; see below. The truth value of a **variable proposition** depends on the value of the variable.

Truth table for $\wedge$ (and)

p	q	$p \wedge q$
true	true	true
true	false	false
false	true	false
false	false	false

Truth table for $\vee$ (inclusive or)

p	q	$p \vee q$
true	true	true
true	false	true
false	true	true
false	false	false

Truth table for $\Rightarrow$ (implication)

p	q	$p \Rightarrow q$
true	true	true
true	false	false
false	true	true
false	false	true

Modus Ponens

From knowledge that the propositions

p and $p \Rightarrow q$

are both true, we can deduce that

q is true.

Mathematical induction (generalised version)

Let N be a natural number, and let $p(n)$ be a variable proposition. If
(a) $p(N)$ is true, and
(b) the implication $p(k) \Rightarrow p(k+1)$ is true for all $k \geq N$,
then we can deduce that

$p(n)$ is true for all $n \geq N$.

An example of proof by mathematical induction

Prove that, for all $n \geq 5$,

$2^n > 4n$.

Proof

Let $p(n)$ be the variable proposition: $2^n > 4n$.

With $n = 5$, we have $2^5 = 32$ and $4 \times 5 = 20$. Since $32 > 20$ is true, $p(5)$ is true.

Establish the starting point N, which is 5 in this example.

Now suppose that $p(k)$ is true, where $k \geq 5$. Then $2^k > 4k$, so

$$\begin{aligned} 2^{k+1} - 4(k+1) &= 2 \times 2^k - 4(k+1) \\ &> 2 \times 4k - 4(k+1), \quad \text{since } 2^k > 4k, \\ &= 4k - 4. \end{aligned}$$

Suppose that the result holds for $n = k, \ldots$

Now $4k - 4 > 0$ for $k > 1$, so $2^{k+1} > 4(k+1)$.

... and show that it must then hold for $n = k + 1$.

Thus we have shown that if $p(k)$ is true, where $k \geq 5$, then $p(k+1)$ is also true.

Thus the proposition $p(k) \Rightarrow p(k+1)$ is true for $k \geq 5$.

Thus we deduce by mathematical induction that $p(n)$ is true for all $n \geq 5$.

Deduce by mathematical induction that $p(n)$ is true for all $n \geq 5$.

The Open University
ISBN 0 7492 6647 3